(19)日本国特許庁（ＪＰ）　**再公表特許（Ａ１）**　(11)国際公開番号

ＷＯ０１／０４６８０８

発行日　平成15年６月10日(2003.6.10)　(43)国際公開日　平成13年６月28日(2001.6.28)

(51)Int.Cl.[7]		識別記号	FI		
Ｇ０６Ｆ	12/16	３１０	Ｇ０６Ｆ	12/16	３１０Ｍ
	3/06	５４０		3/06	５４０
	12/14	３２０		12/14	３２０Ａ
	15/00	３１０		15/00	３１０Ｕ
Ｈ０４Ｌ	9/28		Ｈ０４Ｌ	9/00	６６１

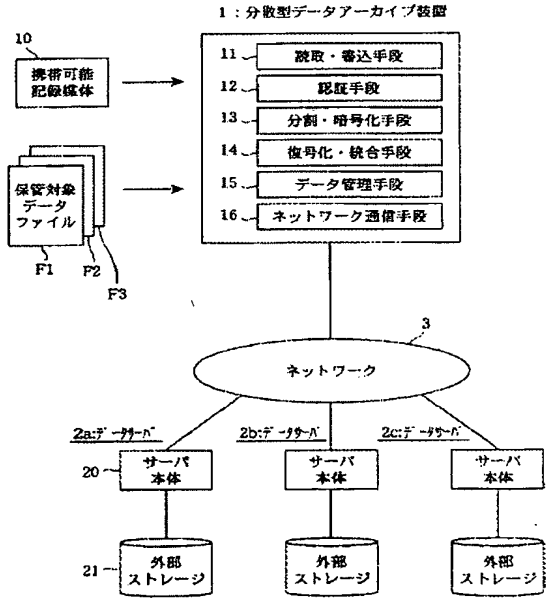
審査請求　有　　予備審査請求　未請求(全 75 頁)　最終頁に続く

出願番号　特願2001－547256(P2001－547256)
(21)国際出願番号　ＰＣＴ／ＪＰ００／０８９８６
(22)国際出願日　平成12年12月19日(2000.12.19)
(31)優先権主張番号　特願平11－360273
(32)優先日　平成11年12月20日(1999.12.20)
(33)優先権主張国　日本（ＪＰ）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ，ＴＲ)，ＡＵ，ＣＡ，ＣＮ，ＪＰ，ＫＲ，ＳＧ，ＵＳ

(71)出願人　大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(72)発明者　矢野　義博
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　大島　直行
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(72)発明者　半田　富己男
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内
(74)代理人　弁理士　志村　浩

(54)【発明の名称】　分散型データアーカイブ装置およびシステム

(57)【要約】
ネットワーク（３）上の任意の場所に、分散型データアーカイブ装置（１）を設け、データの保管および取出しができるようにする。データ保管時には、保管対象データファイル（Ｆ１）をアーカイブ装置（１）に与えると、分割・暗号化手段（１３）によって分割暗号化が行われ、ネットワーク通信手段（１６）によって、個々の分割ファイルが各データサーバ（２ａ，２ｂ，２ｃ）に分散されて保管される。データ管理手段（１５）は、この保管時に行われた分割方法および暗号化方法、並びに保管先データサーバを示す管理データを作成し、携帯可能記録媒体（１０）に記録する。データ取出時には、携帯可能記録媒体（１０）を任意のアーカイブ装置（１）に接続し、管理データを読出し、この管理データに基づいて、各保管先から分割ファイルを取出し、復号化・統合手段（１４）によって元のデータファイル（Ｆ１）に復元する。



【特許請求の範囲】

【請求項１】　ネットワーク（３）を介してアクセス可能な複数のデータサーバ（２ａ，２ｂ，２ｃ）に、保管対象データ（Ｆ１）を分散して保管する機能と、保管されていたデータを必要に応じて取出す機能と、を有する分散型データアーカイブ装置（１）であって、

データ保管時に、保管対象データ（Ｆ１）を所定の分割方法に基づいて複数の分割ファイル（Ｆ１１，Ｆ１２，Ｆ１３）に分割する分割手段（１３）と、

データ取出時に、前記分割方法を考慮して前記複数の分割ファイルを統合して元の保管対象データに復元する統合手段（１４）と、

データ保管時には、前記複数の分割ファイルを、前記ネットワークを介してそれぞれ所定のデータサーバへ転送して保管させる処理を行い、データ取出時には、前記ネットワークを介して個々のデータサーバに保管されている前記複数の分割ファイルを取出す処理を行うネットワーク通信手段（１６）と、

データ保管時には、前記分割手段によって採られた分割方法を示す情報を含んだデータ保管時の手順を示すデータ保管手順情報と、前記ネットワーク通信手段によって転送された複数の分割ファイルの保管先となるデータサーバを特定するデータ保管場所情報と、を有する管理データを作成し、この管理データを所定の場所に記録する処理を行い、データ取出時には、前記管理データを読み出し、この管理データに含まれている前記データ保管手順情報を前記統合手段に与え、この管理データに含まれている前記データ保管場所情報を前記ネットワーク通信手段に与える処理を行うデータ管理手段（１５）と、

を備えることを特徴とする分散型データアーカイブ装置。

【請求項２】　請求項１に記載の分散型データアーカイブ装置において、

携帯可能記録媒体（１０）に対して、データの読み書きを行う機能をもった読取・書込手段（１１）を更に備え、データ管理手段（１５）が、前記読取・書込手段を介して前記携帯可能記録媒体内に管理データを記録する処理を行うことを特徴とする分散型データアーカイブ装置。

【請求項３】　請求項１に記載の分散型データアーカイブ装置において、

所定の場所に記録されている管理データをアクセスするために必要なアクセス

情報が格納された携帯可能記録媒体（１０）に対して、データの読み書きを行う機能をもった読取・書込手段（１１）を更に備え、データ管理手段（１５）が、前記読取・書込手段を介して前記携帯可能記録媒体内の前記アクセス情報を読み出し、このアクセス情報に基づいて管理データへのアクセスを行うことを特徴とする分散型データアーカイブ装置。

【請求項４】　請求項１～３のいずれかに記載の分散型データアーカイブ装置において、

利用者の正当性を検査する認証手段（１２）を更に備え、正しい認証結果が得られた場合にのみ、データ保管処理もしくはデータ取出処理が実行されるようにしたことを特徴とする分散型データアーカイブ装置。

【請求項５】　請求項１～４のいずれかに記載の分散型データアーカイブ装置において、

分割手段が、保管対象データを分割する処理を行うプロセスにおいて、データに対する暗号化処理を行う分割・暗号化手段（１３）として機能し、

データ管理手段（１５）が、前記暗号化処理の方法を示す情報を含んだデータ保管手順情報を作成して、これを管理データとして記録する機能を果たし、

統合手段が、分割ファイルを統合して元の保管対象データに復元する際に、前記データ保管手順情報に含まれている前記暗号化処理の方法を示す情報に基づいて、暗号化された部分に対する復号化処理を行う復号化・統合手段（１４）として機能するようにしたことを特徴とする分散型データアーカイブ装置。

【請求項６】　請求項５に記載の分散型データアーカイブ装置において、

データ管理手段（１５）が、暗号化処理の方法を示す情報の一部として、分割処理と暗号化処理とについての実行順を示す情報を用いることを特徴とする分散型データアーカイブ装置。

【請求項７】　請求項１～６のいずれかに記載の分散型データアーカイブ装置において、

分割手段（１３）が、保管対象データを分割する処理を行うプロセスにおいて、前記保管対象データとは無関係なダミーデータを付加する処理を行うようにし

データ管理手段（１５）が、ダミーデータ付加処理に関する情報を含んだデータ保管手順情報を作成して、これを管理データとして記録する機能を果たし、

統合手段（１４）が、分割ファイルを統合して元の保管対象データに復元する際に、前記データ保管手順情報に含まれている前記ダミーデータ付加処理に関する情報に基づいて、付加されていたダミーデータの除去処理を行うようにしたことを特徴とする分散型データアーカイブ装置。

【請求項８】　請求項１～７のいずれかに記載の分散型データアーカイブ装置において、

分割手段（１３）が、保管対象データを分割して複数の分割ファイルを作成する処理を行うプロセスにおいて、前記保管対象データに冗長度を付加して保管するために必要な冗長格納処理を行うようにし、

データ管理手段（１５）が、前記冗長格納処理に関する情報を含んだデータ保管手順情報を作成して、これを管理データとして記録する機能を果たし、

統合手段（１４）が、前記データ保管手順情報に含まれている前記冗長格納処理に関する情報を考慮して、元の保管対象データを復元する処理を行うようにしたことを特徴とする分散型データアーカイブ装置。

【請求項９】　請求項１～８のいずれかに記載の分散型データアーカイブ装置において、

データ保管時に、期間に関する制限を示す期間制限情報を、保管対象データに付加した上で、データサーバに分散して保管する機能を更に設け、

データ取出時に、前記期間制限情報に基づく制限を考慮した取出処理が行われるようにしたことを特徴とする分散型データアーカイブ装置。

【請求項１０】　請求項１～９のいずれかに記載の分散型データアーカイブ装置において、

データ保管時に、各データサーバに分散して保管される個々の分割ファイルに、本来の保管先とは異なる退避先を示す退避先情報を付加するとともに、この退避先情報を管理データの一部として記録する機能を更に設け、

データ取出時に、本来の保管先となるデータサーバから所望の分割ファイルを取出すことができない場合には、前記退避先情報によって示された退避先となる

データサーバから前記所望の分割ファイルを取出す処理が行われるようにしたことを特徴とする分散型データアーカイブ装置。

【請求項１１】 請求項１～１０のいずれかに記載の分散型データアーカイブ装置（１）と、この分散型データアーカイブ装置が接続されたネットワーク（３）と、このネットワーク（３）を介して前記分散型データアーカイブ装置からのアクセスを受ける複数のデータサーバ（２ａ，２ｂ，２ｃ）と、「前記分散型データアーカイブ装置内で作成された管理データ」もしくは「この管理データをアクセスするために必要な情報」の記録場所として利用される携帯可能記録媒体（１０）と、を備えることを特徴とする分散型データアーカイブシステム。

【請求項１２】 請求項１１に記載の分散型データアーカイブシステムにおいて、

ネットワークに接続された端末装置が、分散型データアーカイブ装置（１）としての機能とデータサーバ（２ａ，２ｂ，２ｃ）としての機能とを兼ね備えるようにし、用途に応じてこれら２つの機能を選択可能な構成としたことを特徴とする分散型データアーカイブシステム。

【請求項１３】 請求項１１または１２に記載の分散型データアーカイブシステムにおいて、

携帯可能記録媒体（１０）としてＩＣカードを用い、分散型データアーカイブ装置（１）が前記携帯可能記録媒体にアクセスを行う際には、当該携帯可能記録媒体自体の正当性検査を行うようにしたことを特徴とする分散型データアーカイブシステム。

【請求項１４】 請求項１１～１３のいずれかに記載の分散型データアーカイブシステムにおいて、

複数の携帯可能記録媒体（１０）に、同一の管理データをアクセスするために必要な情報が格納されていることを特徴とする分散型データアーカイブシステム。

【請求項１５】 請求項１１～１４のいずれかに記載の分散型データアーカイブシステムにおいて、

分散型データアーカイブ装置（１）が、データ保管時に、各データサーバ（２

ａ，２ｂ，２ｃ）に分散して保管される個々の分割ファイルに、本来の保管先とは異なる退避先を示す退避先情報を付加する機能を有し、

データサーバ（２ａ，２ｂ，２ｃ）が、分割ファイルの保管を継続することに支障が生じた場合に、保管中の分割ファイルを前記退避先情報によって示されている退避先となる別なデータサーバに退避させる処理を行う機能を有することを特徴とする分散型データアーカイブシステム。

【請求項１６】 請求項１～１０のいずれかに記載の分散型データアーカイブ装置を実現するプログラムを記録したコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

技 術 分 野

本発明は、デジタルデータを、ネットワークを利用して所定の場所に保管し、必要なときにこれを取り出すことが可能なデータアーカイブ装置およびデータアーカイブシステムに関する。特に、本発明は、バックアップの目的で、貴重なデジタルデータの複製を、ネットワーク上の複数の箇所に分散して保管することができるデータアーカイブシステムに関する。

背 景 技 術

データを作成したコンピュータ等から、ネットワークで接続されている他のファイルサーバ等に、作成したデータのバックアップデータを転送し、貴重なデータの保管を行うことは広く行われている。このネットワークを、たとえば、インターネットのような世界的規模の広域ネットワークにまで拡張すれば、インターネットにアクセスすることができる環境さえあれば、世界中のどこからでもデータの保管を行うことができ、保管されていたデータを世界中のどこからでも取り出すことができる。しかしながら、利用するネットワークの規模を拡大すればするほど、利用者の利便性は向上するが、逆にセキュリティは低下することになる。保管対象となるデータは、通常、個人個人のプライベートな情報を含んでおり、データを預けた本人あるいは本人の委託を受けた代理人だけが取り出せるよう、十分なセキュリティを確保しておく必要がある。このように、ネットワークを利用した従来のデータアーカイブシステムには、どこからでもデータの預け入れや取り出しができるように利便性を向上させると、セキュリティが低下するという問題が生じていた。

本発明はこのような問題を考慮してなされたものであり、データを預けた本人あるいはデータへのアクセスを許可された特定の者だけが、任意の場所から預け入れたデータに安全にアクセスでき、しかもデータを保管するサーバ側に特別な装置やソフトウエアの用意を必要としないデータアーカイブシステムを提供することを目的とする。

発 明 の 開 示

上記課題を解決するために、本発明は、利用者の正当性検査を行う認証手段と

、保管対象データを複数の部分に分割する分割手段と、分割保管されたデータを元の単一データファイルに復元する統合復元手段と、保管対象データを納めたデータサーバとの間で定められた通信プロトコルにより、分割されたデータファイルを転送するネットワーク通信手段と、新規にデータ保管を行う時に、保管対象データの保管場所を示すデータ保管場所情報および保管対象データの分割方法等を示すデータ保管手順情報を記録するデータ管理手段と、を備えた分散型データアーカイブ装置を用意し、保管対象データを保管する際には、これを複数の部分に分割し、分割された個々の部分毎にネットワーク上の複数のサーバに転送して分散保管させ、保管対象データを取り出す際には、保管時に記録されたデータ保管場所情報およびデータ保管手順情報にしたがって、ネットワーク上の複数のサーバに分散して保管されている保管対象データを取り出し、これを合成して元のファイルに復元して利用者に提供するようしたものである。データを分割して複数のサーバに保管すれば、貴重なデータの盗み出しは困難である。

また、上記課題を解決するために、本発明は、携帯可能記録媒体に対してデジタルデータの書込みおよび読み出しを行う機能をもった読取・書込手段と、利用者の正当性検査を行う認証手段と、保管対象データを複数の部分に分割する分割手段と、分割保管されたデータを元の単一データファイルに復元する統合復元手段と、保管対象データを納めたデータサーバとの間で定められた通信プロトコルにより、分割されたデータファイルを転送するネットワーク通信手段と、新規にデータ保管を行う時に、保管対象データの保管場所を示すデータ保管場所情報および保管対象データの分割方法等を示すデータ保管手順情報を、前記携帯可能記録媒体に記録するデータ管理手段と、を備えた分散型データアーカイブ装置を用意し、この分散型データアーカイブ装置と、前記携帯可能記録媒体と、ネットワークと、複数のデータサーバと、によって、分散型データアーカイブシステムを構成し、保管対象データを保管する際には、前記携帯可能記録媒体に記録したデータ保管場所情報およびデータ保管手順情報にしたがって、この保管対象データを複数の部分に分割し、分割された個々の部分毎にネットワーク上の複数のサーバに転送して分散保管させ、保管対象データを取り出す際には、前記携帯可能記録媒体に記録されたデータ保管場所情報およびデータ保管手順情報にしたがって

、ネットワーク上の複数のサーバに分散して保管されている保管対象データを取り出し、これを合成して元のファイルに復元して利用者に提供するようしたものである。このシステムでは、前記携帯可能記録媒体を携帯していれば、ネットワークに接続された任意の分散型データアーカイブ装置から保管データにアクセスすることが可能となる。たとえば、利用者は、データ保管場所情報およびデータ保管手順情報を記録した、フロッピー（登録商標）ディスクのような記録媒体を携帯していれば、ネットワークに接続された任意の分散型データアーカイブ装置にログインすることにより、どこからでも所望のアーカイブデータを取り出すことができる。

更に、データを暗号化する手段を付加し、分割手段によって保管対象データを分割した後に暗号化するか、または保管対象データに暗号化を施した後に分割して、保管すべき複数の分割データを作成するようにし、データ管理手段によって、暗号化や復号化に必要な暗号鍵情報等をデータ保管手順情報として記録するようにし、統合復元手段は、記録されているデータ保管手順情報に従って、保管されていた個々の分割データを復号化してから統合化するか、または先に統合してから復号化するかして、元のデータに復元するようにすると、より強力な効果を奏する。個々の分割データを暗号化すれば、元のデータを知ることは困難であり、インターネットのようなオープンなネットワーク上でデータを保管しても、データを取り出す時に盗み見される心配は実質的に無い。

また、データの保管時に、保管対象データを分割したり、分割した後に暗号化したり、または暗号化して後に分割したりする際に、いずれかの段階において、一定の規則に従ってダミーデータを付加するようにし、データ管理手段によって、このダミーデータ付加規則をデータ保管手順情報として記録しておくようにし、データの取出時には、データ保管手順情報に従って、保管されていた分割データに対する統合化や復号化処理を行う際の所定の段階において、保管時に付加されたダミーデータを除去するようにすれば、保管されていたデータを盗み見されたり、これを復号化されたとしても、ダミーデータが介在しているために完全な復元には至らないので、保管されていたデータを盗まれた場合の安全性が更に高まる。

更に、分割したデータを冗長性を持たせて複数のデータサーバに保管しておくようにすれば、どれか１つのデータサーバがダウンしても、他の正常なサーバのデータだけから元のデータを復元できるようになる。データサーバ自体がダウンすることも考慮すると、このような分散型データアーカイブシステムはより安全である。

また、上述した携帯可能記録媒体としては、セキュリティの高いＩＣカードを用いることがより望ましい。こうすることにより、記録されているデータ保管場所情報やデータ保管手順情報の読み出し、コピーなどがより困難となり、ＩＣカード所有者だけが保管されているデータにアクセスできることになる。

また、上記分散型データアーカイブ装置は、汎用のコンピュータに、専用のプログラムを組み込むことにより実現することができ、そのような専用のプログラムは、コンピュータ読取り可能な記録媒体に記録して配付することができる。ネットワークを介してデータサーバに接続することができる任意の汎用コンピュータに、上記専用プログラムを組み込めば、当該汎用コンピュータを本発明に係る分散型データアーカイブ装置として利用することができるようになり、携帯可能記録媒体を携帯している限り、実質的に任意の場所から保管されたデータにアクセスすることができる。

発明を実施するための最良の形態

§１．基本的な実施形態

まず、本発明の基本的な実施形態を説明する。図１は、本発明に係る分散型データアーカイブシステムの全体構成図である。分散型データアーカイブ装置１は、この分散型データアーカイブシステムの中枢をなす装置であり、複数のデータサーバ２（図１では２ａ，２ｂ，２ｃ）に対して、ネットワーク３を介して、所望のデータを保管する機能を有している。この分散型データアーカイブ装置１には、携帯可能記録媒体１０を挿入することができ、上記機能を実行する際には、分散型データアーカイブ装置１と携帯可能記録媒体１０との連携動作が行われる。分散型データアーカイブ装置１は、図１に示されているように、読取・書込手段１１、認証手段１２、分割・暗号化手段１３、復号化・統合手段１４、データ管理手段１５、ネットワーク通信手段１６から構成される。これら各手段の個々

の機能については後述する。利用者が、この図１に示されたデータアーカイブシステムを利用してデータを保管するには、保管対象となるデータを、ファイル単位で分散型データアーカイブ装置１に与えればよい。図１には、保管対象データファイルとして、３つのファイルＦ１、Ｆ２、Ｆ３を分散型データアーカイブ装置１に与えた例が示されている。この分散型データアーカイブ装置１は、具体的には、携帯可能記録媒体１０用のドライブ装置を備えた汎用コンピュータに、後述する機能を実現する専用のソフトウエアプログラムを組み込むことにより実現できる。一方、個々のデータサーバ２は、それぞれサーバ本体２０と外部ストレージ２１とによって構成される。保管対象となるデータは、個々のファイルごとに、ネットワーク３を経由して、複数のデータサーバ２ａ、２ｂ、２ｃに、所定のデータ保管手順にしたがって保管される。

携帯可能記録媒体１０には、データサーバ２ａ、２ｂ、２ｃに保管された個々のファイル（図示の例の場合、Ｆ１、Ｆ２、Ｆ３）ごとに、データ保管場所およびデータ保管手順を示す管理データが格納される。図２は、携帯可能記録媒体１０の中に記録されている管理データの一例を示す図である。１つの携帯可能記録媒体１０内には、所定のパスワードの入力によりアクセスが可能となる管理フォルダが作成されており、この管理フォルダ内には、個々のファイルの管理データを格納するためのフォルダが更に作成されている。たとえば、図２に示す例では、管理フォルダ内に、Ｆ１用フォルダ、Ｆ２用フォルダ、Ｆ３用フォルダと記述された３つのフォルダが作成されており、これら各フォルダ内には、それぞれファイルＦ１の管理データ、ファイルＦ２の管理データ、ファイルＦ３の管理データが格納されている。図２には、このうちのファイルＦ１の管理データの内容が例示されている。各管理データは、各ファイルを構成するデータの保管場所を示すデータ保管場所情報と、データの保管手順を示すデータ保管手順情報と、によって構成されている。本発明では、保管対象となる１つのデータファイルは、複数に分割され、複数のデータサーバに分散して保管されることになる。データ保管場所情報は、保管対象となるデータファイルの保管先となっている複数のデータサーバの場所を示す情報であり、具体的には、保管先となっている複数のデータサーバのアドレス（Ｕｎｉｆｏｒｍ Ｒｅｓｏｕｒｃｅ Ｌｏｃａｔｏｒ、以

下ＵＲＬという）のリストから構成される。

一方、データ保管手順情報は、図示の例の場合、「分割方法」、「暗号化方法」、「分割・暗号化の順番」、「冗長格納方法」、「ダミーデータ付加方法」なる各項目を示す情報（識別文字、数字、条件式など）によって構成される。ここで、「分割方法」なる項目については、更に、「ファイル分割アルゴリズム」、「分割ファイルサイズ」、「分割ファイル数」という細かな項目が設定されている。たとえば、保管対象となる１つのデータファイルＦ１を保管する場合、このデータファイルＦ１を複数のファイルに分割することになるが、どのような方法で分割を行うかという情報が、上述した「分割方法」なる項目に管理データとして格納されることになる。より詳細には、どのような「ファイル分割アルゴリズム」を用いて分割を行い、個々の「分割ファイルサイズ」をどのように設定し、「分割ファイル数」はいくつになったか、という情報が、個々の細目に格納される。

また、保管対象となるデータファイルＦ１に対して暗号化を施した場合には、どのような方法で暗号化を行ったかを示す情報が、上述した「暗号化方法」なる項目に管理データとして格納され、分割処理前のもとのデータファイルＦ１に対して暗号化を行った後、この暗号化されたデータに対して分割処理を行ったのか、あるいは、先に分割処理を行った後に、個々の分割ファイルに対して暗号化処理を行ったのか、を示す情報が、上述した「分割・暗号化の順番」なる項目に管理データとして格納される。

更に、個々の分割ファイルを各データサーバに保管する際に、冗長性をもたせて格納を行う場合には、採用した冗長格納方法を示す情報が、上述した「冗長格納方法」なる項目に管理データとして格納されることになる。一般的な冗長格納方法としては、ミラーリング方式と、パリティファイル作成方式の２通りが知られている。ミラーリング方式を採る場合には、各分割ファイルごとに、それぞれ正と副の２か所の異なるデータサーバに重複した保管が行われる。万一、一方の分割ファイルが滅失したとしても、もう一方の分割ファイルさえ残っていれば、危険は回避できる。一方、パリティファイル作成方式を採る場合は、たとえば、互いにデータ長の等しい一対の分割ファイルについて、各ビットごとに排他的論

理和をとることによりパリティファイルを作成し、このパリティファイルと一対の分割ファイルとを、それぞれ所定のデータサーバに格納することになる（一般に、ＲＡＩＤ３と呼ばれる方式の例）。万一、一方の分割ファイルが滅失したとしても、対となるもう一方の分割ファイルとパリティファイルとについて、各ビットごとに排他的論理和をとれば、滅失した分割ファイルを復元できる。

また、保管対象となるデータファイルＦ１を分割する処理を行うプロセスにおいて、このファイルＦ１内のデータとは無関係なダミーデータを付加する処理を行った場合には、どのような方法でダミーデータを付加したかを示す情報が、上述した「ダミーデータ付加方法」なる項目に管理データとして格納されることになる。たとえば、ランダムな任意のデータを発生させて、これをダミーデータとして利用することもできるし、予め用意しておいた何らかのデータをダミーデータとして利用してもよい。このようなダミーデータを付加しておけば、万一、分割ファイルが不正な手段で閲覧された場合にも、閲覧内容を撹乱することができ、セキュリティを向上させることができる。もちろん、ダミーデータは、本来のデータのどの部分に付加してもかまわない。たとえば、保管対象となるデータファイルＦ１を分割することによって得られた個々の分割ファイルの先頭や末尾などの特定の場所に数バイトのダミーデータを付加してもよいし、先頭から３バイト目ごとに１バイトのダミーデータを挿入する、というような特定の規則で、ところどころにダミーデータを付加してもよい。「ダミーデータ付加方法」なる項目に管理データとして格納される情報は、どのような方法でダミーデータが付加されたか、ということを示す情報であり、後にデータの取出しを行うときに、ダミーデータを除去するプロセスを行うために参照される。

図２には示されていないが、データファイルＦ２，Ｆ３についても、同様に管理データが作成され、携帯可能記録媒体１０内の管理フォルダ内に格納されることになる。このように、本発明に係るデータアーカイブシステムを利用して、３つのデータファイルＦ１，Ｆ２，Ｆ３を保管したとすると、これら各データファイルはいずれも複数の分割ファイルに分割され、個々の分割ファイルはいずれかのデータサーバに保管されることになる。たとえば、データファイルＦ１が、４つの分割ファイルＦ１１～Ｆ１４に分割されたとすると、これら各分割ファイル

Ｆ１１～Ｆ１４は、図１に示す３つのデータサーバ２ａ～２ｃのいずれかに分散して格納される。この際、もとのデータファイルＦ１をどのような方法で分割し、各分割ファイルのサイズは何バイトであり、合計いくつの分割ファイルが作成されたか、という情報は、図２に示す管理フォルダ内にファイルＦ１の管理データ（データ保管手順情報）として格納されることになる。このときに、暗号化、冗長格納、ダミーデータ付加などの方法を採用した場合には、これらの方法に関する情報も管理データとして格納される。そして、この４つの分割ファイルＦ１１～Ｆ１４が、それぞれどのデータサーバに格納されるかを示す情報（個々のデータサーバのＵＲＬリスト）が、図２に示す管理フォルダ内にファイルＦ１の管理データ（データ保管場所情報）として格納される。

なお、保管対象となるデータファイルに基づいて作成される個々の分割ファイルには、それぞれ所定の規則に従ってユニークなファイル名が付与されるようにしておき、かつ、元のデータファイルとの対応関係が明らかになるようにしておく。たとえば、上述の例の場合、保管対象となるデータファイルのファイル名が「Ｆ１」であったとすると、このデータファイル「Ｆ１」に基づいて作成される個々の分割ファイルの名は、「Ｆ１」の末尾にそれぞれ１～４の数字を付加する、という規則に従って、「Ｆ１１」～「Ｆ１４」なる名が付与されることになる。ここで、たとえば、図２に示す「Ｆ１用フォルダ」のフォルダ名を、データファイルＦ１と同じ「Ｆ１」なる名称にしておき、このフォルダ「Ｆ１」内に記録されるファイル「Ｆ１」の管理データのデータ保管場所情報には、個々の分割ファイル名「Ｆ１１」～「Ｆ１４」のそれぞれについて、保管先となったデータサーバのＵＲＬを対応づけるリスト（具体的には、Ｆ１１→ＵＲＬ（２ａ），Ｆ１２→ＵＲＬ（２ｂ），．．．というようなリスト）を記録するようにしておけば、保管対象となるデータファイルのファイル名「Ｆ１」と、個々の分割ファイルのファイル名「Ｆ１１」～「Ｆ１４」との対応関係が、図２に示すファイル構造によって明記されることになる。もっとも、インターネットでは、通常、ｈｔｔｐ：／／ｗｗｗ．（サーバ特定コード）／（ファイル特定コード）のような形式のＵＲＬが利用されているので、実用上は、データ保管場所情報としては、Ｆ１１→ＵＲＬ（２ａ）．Ｆ１２→ＵＲＬ（２ｂ）．．．．というような対応関係を

示すリストではなく、ｈｔｔｐ：／／ｗｗｗ．（データサーバ２ａ）／（分割ファイルＦ１１），ｈｔｔｐ：／／ｗｗｗ．（データサーバ２ｂ）／（分割ファイルＦ１２），．．．というようなＵＲＬリストを用意しておくと便利である。

以上のような手順でデータファイルＦ１を保管しておけば、管理フォルダ内に格納されているファイルＦ１の管理データ（データ保管手順情報とデータ保管場所情報）を用意して、このデータアーカイブシステムにアクセスすることができれば、いつでも、どこからでも、保管されているデータファイルＦ１を取り出すことができる。すなわち、ファイルＦ１の管理データ内のデータ保管場所情報（データサーバのＵＲＬリスト）を参照すれば、どこのデータサーバに必要な分割ファイルが保管されているかを認識することができるので、復元に必要な分割ファイルをすべて読み出してくることができる。しかも、ファイルＦ１の管理データ内のデータ保管手順情報を参照すれば、読み出してきた各分割ファイルに対して、どのような復号化を行い、どの部分をダミーデータとして削除し、どのようなファイル統合を行えば、もとのデータファイルＦ１を得ることができるか、という復元手順を認識することができるので、この復元手順に従って、もとのデータファイルＦ１を復元することができる。すなわち、保管データの取出処理を行うことができる。

図１に示す分散型データアーカイブ装置１内に示された各手段１１～１６は、上述したような、データファイルの保管処理と、保管データの取出処理とを行う機能を有している。すなわち、読取・書込手段１１は、携帯可能記録媒体１０内の管理フォルダにアクセスする手段であり、個々のファイルごとの管理データを読み書きする機能を果たす。また、認証手段１２は、携帯可能記録媒体１０自体の正当性検査を行うとともに、管理フォルダにアクセスするために必要なパスワードの入力を確認することにより、利用者に対する認証を行う機能を果たす。分割・暗号化手段１３は、保管対象となる特定のデータファイルについて、保管処理を行う旨の指示が与えられたときに、予め定められた規則に従って、このデータファイルを所定の分割方法に基づいて分割し、必要に応じて暗号化、ダミーデータ付加、冗長格納のための処理を実行し、個々の分割ファイルごとに保管先となるデータサーバを決定する機能を果たす。

これに対して、復号化・統合手段１４は、保管されている特定のデータファイルについて、取出処理を行う旨の指示が与えられたときに、当該特定のデータファイルについての保管時の処理手順を示す管理データに基づいて、分割ファイルの統合、復号化、ダミーデータの削除を行う機能を果たす。また、データ管理手段１５は、保管処理を行う旨の指示が与えられたときには、分割・暗号化手段１３によって実行される処理手順や各分割ファイルの保管先を示す管理データ（データ保管手順情報とデータ保管場所情報）を作成し、読取・書込手段１１を介して、この管理データを携帯可能記録媒体１０内の管理フォルダに書込む機能を果たす。一方、このデータ管理手段１５は、取出処理を行う旨の指示が与えられたときには、読取・書込手段１１を介して、携帯可能記録媒体１０内の管理フォルダから必要な管理データを読み出し、これを復号化・統合手段１４やネットワーク通信手段１６に伝達する処理を行う。また、このデータ管理手段１５は、読取・書込手段１１を介して、携帯可能記録媒体１０内の管理フォルダにアクセスし、その内容を利用者に提示する機能も有している。最後のネットワーク通信手段１６は、インターネットの標準技術であるファイルトランスファプロトコル（Ｆｉｌｅ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ、以下ＦＴＰという）を利用して、各分割ファイルをネットワーク３を介して所定のデータサーバに転送して格納したり、逆に、所定のデータサーバから分割ファイルを読み出したりする機能を果たす。

このような各手段１１～１６によって構成される分散型データアーカイブ装置１を、ネットワーク３上の随所に設置しておくようにすれば、携帯可能記録媒体１０を携帯している利用者は、このデータアーカイブ装置１の設置場所であれば、どこでも、いつでも、任意のデータファイルを保管することが可能になり、また、保管しておいた任意のデータファイルを取り出すことが可能になる。ネットワーク３としてインターネットを利用すれば、データアーカイブ装置１が設置してある場所であれば、世界中のどこからでも、データを保管する作業を行うことができ、保管したデータを取り出す作業を行うことができる。このように、携帯可能記録媒体１０さえ携帯していれば、どこでも、いつでも、データファイルの出し入れができる、という点が、本発明に係るデータアーカイブシステムの第１

のメリットである。この第１のメリットは、天災や事故などに対する保管データの安全性向上にもつながることになる。たとえば、保険会社や金融機関などでは、貴重な業務データを安全に保管するための対策を講じておく必要がある。本発明に係るシステムを利用すれば、保管対象となるデータを世界各地に分散して保管しておくことが可能になり、局所的な災害や事故などに対する耐久性の高いデータアーカイブシステムが実現できる。

本発明に係るデータアーカイブシステムの第２のメリットは、データサーバ側に特別な対策を施さなくても、十分なセキュリティが確保できるという点である。図１に示すシステムにおいて、インターネットをネットワーク３として利用したとすると、利用者の利便性は向上するものの、各データサーバ２ａ～２ｃのセキュリティは必ずしも万全とは言えず、不正なアクセスによって、各データサーバ内に保管しておいたデータが閲覧されてしまう可能性がある。しかしながら、本発明に係るデータアーカイブシステムでは、保管対象となるデータファイルは、保管時に複数の分割ファイルに分けられ、複数のデータサーバに分散して保管されることになるので、個々の分割ファイル単独では本来の情報を構成しないことになる。したがって、各データサーバ内に保管されている個々の分割ファイルが、不正な手段で閲覧されたとしても、セキュリティ上の問題は生じない。通常、業務データをバックアップする場合、バックアップ先となるデータサーバには十分なセキュリティ対策を施す必要があり、バックアップのためのコストが高騰する要因となっている。本発明に係るシステムでは、個々のデータサーバ側には特別なセキュリティ対策を施す必要がないため、バックアップのためのコストを低減させることが可能になる。

もっとも、個々の分割ファイルが、ある程度のデータ長を有していると、断片的ではあるにせよ、不正アクセスによって何らかの意味のある情報が漏れてしまうおそれがある。したがって、実用上は、たとえば、３つの分割ファイルを作成するのであれば、３バイト目おきに１バイトずつ採取したデータによって１つの分割ファイルを構成するなど、分割方法を工夫するようにして、１つの分割ファイルだけを閲覧しても、元のファイルの内容が察知されないようにするのが好ましい。更にセキュリティを高めるためには、上述した実施形態でも述べたように

、分割を行う前、あるいは分割後に、所定のアルゴリズムに基づく暗号化やダミーデータの付加を行うようにするのが好ましい。

また、携帯可能記録媒体１０内に格納されている各ファイルごとの管理データは、各ファイルを取り出すために必要な情報であり、この管理データそのものが盗まれると、保管しておいたデータファイルが不正アクセスによって取り出されてしまうことになる。したがって、実用上は、携帯可能記録媒体１０としては、記録内容が不正アクセスを受けにくい媒体を用いるのが好ましい。具体的には、たとえば、ＣＰＵを内蔵したＩＣカード（以下アーカイブカードという）を携帯可能記録媒体１０として用いると、十分なセキュリティを確保することができる。セキュリテイを更に高める上では、上述した実施形態でも述べたように、携帯可能記録媒体１０内の管理フォルダをアクセスするために、パスワードを要求するような設定にしておくのが好ましい。

§２．具体的な動作手順

続いて、本発明に係る分散型データアーカイブ装置の動作手順の一例を述べる。図３は、分散型データアーカイブ装置１の動作の流れを示す流れ図である。以下、この流れ図に従って、分散型データアーカイブ装置１の働きを説明する。なお、以下の説明では、携帯可能記録媒体１０は、セキュリティの優れたＩＣカード（アーカイブカード）を用いているものとする。

まず、利用者は、分散型データアーカイブ装置１を起動する。上述したように、実際には、この分散型データアーカイブ装置１は、ＩＣカード用のドライブ装置を有する汎用のコンピュータに、専用のデータアーカイブ用ソフトウエアを組み込むことによって実現される。したがって、分散型データアーカイブ装置１の起動処理は、この汎用のコンピュータ上で、専用のデータアーカイブ用ソフトウエアを起動させる操作ということになる。分散型データアーカイブ装置１が起動すると、ディスプレイ画面上に、アーカイブカード１０の挿入を促すメッセージが表示され、アーカイブカード１０が挿入されるまで待機状態となる。利用者が、アーカイブカード１０を挿入すると、読取・書込手段１１によるアクセスが行われ、認証に必要なデータがやりとりされる。そして、認証手段１２の働きにより、アーカイブカード１０の正当性が検査される一方で、アーカイブカード１０

側では、分散型データアーカイブ装置１の正当性（読取・書込手段１１の正当性）の検査が行われる。ここまでが、図３の流れ図のステップＳ１の手順である。これらの正当性検査技術は当業者においては周知の技術であるので詳細な説明は省略する。

続く、ステップＳ２において、否定的な認証結果が得られた場合、すなわち、挿入されたアーカイブカード１０が正当なアーカイブカードとして認められない物であると判定された場合、あるいは逆に、読取・書込手段１１がアーカイブカード１０側から不正と判定された場合は、ステップＳ３へと進み、挿入されたアーカイブカード１０は排出され、再び、ステップＳ１へと戻り、新たなアーカイブカード１０が挿入されるまで待機状態となる。一方、ステップＳ２において、肯定的な認証結果が得られた場合は、ステップＳ５へと進み、利用者に対してパスワード入力を要求し、本人認証が行われることを条件として、アーカイブカード１０内の管理フォルダの内容がディスプレイ画面上に表示される。すなわち、利用者から入力されたパスワードが、図２に示す管理フォルダについて設定されているパスワードに一致することを確認した上で、管理フォルダ内の内容を読み出し、当該アーカイブカード１０を用いて取り出すことができるファイル名（図２の例の場合、３つのデータファイルＦ１，Ｆ２，Ｆ３）が表示される。また、このとき、利用者からの操作入力を受け付けるための操作メニューも表示され、ステップＳ７において、利用者からの対話的な操作入力（イベントの発生）を待つ状態になる。

この実施形態では、利用者は、表示された操作メニューから４通りの操作入力を選択することができ、この操作入力に応じて、ステップＳ７から各ステップへ分岐が行われる。すなわち、利用者は、保管対象データを新規に保管する保管処理、既に保管されているデータを取り出す取出処理、挿入したアーカイブカード１０を排出させる媒体排出処理、この分散型データアーカイブ装置１の動作を終了する終了処理（具体的には、現在実行中のデータアーカイブ用の専用ソフトウエアを終了する処理）の４通りの操作入力を行うことができ、いずれかの操作入力が与えられた場合には、ステップＳ７においてイベント発生と認識され、それぞれ所定の分岐先へとジャンプすることになる。

ここでは、まず、利用者が保管処理を選択したものとしよう。この場合、まず、ステップＳ１１において、保管対象ファイルを指定する処理が行われる。すなわち、ディスプレイ画面上に保管対象ファイルを指定するためのウインドウが表示されるので、利用者は、そのウインドウから保管対象ファイルを指定する操作を行う。上述したように、この実施形態では、分散型データアーカイブ装置１は、汎用のコンピュータを利用して実現されており、保管対象ファイルは、このコンピュータでアクセス可能な磁気ディスク，光ディスク，光磁気ディスクなどに記録した形態で用意しておけばよい。もちろん、ネットワーク３を介して、外部から保管対象ファイルを分散型データアーカイブ装置１に読み込むようにしてもかまわない。ここでは、たとえば、分散型データアーカイブ装置１を構成するコンピュータのハードディスク装置に格納されていたデータファイルＦ１が、保管対象ファイルとして指定されたものとしよう（この場合、図２に示す「ファイルＦ１の管理データ」はまだ作成されていないことになる。）。

続いて、ステップＳ１３において、「ファイル分割方法」が決定される。具体的には、保管対象ファイルＦ１を、どのような方法で（アルゴリズム）、どのようなファイル長をもった（ファイルサイズ）、いくつのファイル（ファイル数）に分割するか、という条件を定める。これらの条件は、利用者自身によって指定させることも可能であるが、実用上は、分散型データアーカイブ装置１内に予め用意された所定のプログラムに基づいて自動的に決定されるようにするのが好ましい。これらの条件は、セキュリティを高める上では、個々の保管対象ファイルごとに異ならせるようにするのが好ましい。なお、一般的な分割アルゴリズムを用いている場合には、「分割ファイルサイズ」と「分割ファイル数」とは相互に関連あるパラメータとなるので、いずれか一方を決定すると、他方が一義的に決定される。たとえば、保管対象ファイルＦ１のファイル長が１００ＭＢであった場合、「分割ファイルサイズ」を２０ＭＢに決定すれば、「分割ファイル数」は一義的に５に決定されることになるし、「分割ファイル数」を１０に決定すれば、「分割ファイルサイズ」は一義的に１０ＭＢに決定されることになる。

なお、上述の例は、各分割ファイルサイズが互いに等しくなるような等分割を行う分割アルゴリズムを設定した例であるが、ファイル分割アルゴリズムはこの

ような等分割に限定されるものではなく、たとえば、「偶数番目の分割ファイルのファイル長を、奇数番目の分割ファイルのファイル長の２倍に設定する」というような任意の分割アルゴリズムを設定することも可能である。また、ファイルを分割する際には、必ずしも、元のファイルの連続した一部分を１つの分割ファイルとするようなアルゴリズムを採る必要もない。たとえば、１つの保管対象ファイルを２つの分割ファイルに分ける場合、前半部分からなる第１の分割ファイルと後半部分からなる第２の分割ファイルとの２つに分けるアルゴリズムだけでなく、たとえば、奇数番目のバイトからなる第１の分割ファイルと偶数番目のバイトからなる第２の分割ファイルの２つに分けるアルゴリズムも有効である。実用上は、セキュリテイを確保する上で、むしろ後者の分割アルゴリズムを採った方が好ましい。奇数番目のバイトのみからなる分割ファイルや、偶数番目のバイトのみからなる分割ファイルは、通常、それ自身では、全く意味をなさないファイルになるので、不正アクセスによって閲覧されることがあっても、貴重な情報が漏洩することを防ぐことができる。

もちろん、３以上のファイルに分割する場合にも、このような分割アルゴリズムを採ることが可能であり、一般に、ｎ個のファイルに分割するのであれば、分割対象となるファイルを構成する先頭から順に、第１番目のバイトを第１の分割ファイルに、第２番目のバイトを第２の分割ファイルに、．．．、第ｎ番目のバイトを第ｎの分割ファイルに、第（ｎ＋１）番目のバイトを第１の分割ファイルに、第（ｎ＋２）番目のバイトを第２の分割ファイルに、というように割り当ててゆけばよい。もちろん、順に１バイト単位で割り当てる代わりに、順に任意のバイト単位で割り当てることも可能である。実際、ファイル分割のアルゴリズムは無限にあり、どのような分割アルゴリズムを採るようにしてもよい。

次に、ステップＳ１７において、暗号化方法を決定し、続くステップＳ１９において、ダミーデータ付加方法を決定し、更に、ステップＳ２１において、冗長格納方法を決定する。これらの事項も、利用者自身によって指定させることも可能であるが、実用上は、分散型データアーカイブ装置１内に予め用意された所定のアルゴリズムに基づいて自動的に決定されるようにするのが好ましい。また、セキュリティを高める上では、暗号化方法やダミーデータ付加方法を、個々の保

管対象ファイルごとに異ならせるようにするのが好ましく、更に、個々の分割ファイルごとに異ならせるようにするのが好ましい。

ステップＳ１７で決定する事項は、どのようなアルゴリズムで暗号化を行うか、暗号化のプロセスで用いる暗号鍵をどのようなデータにするか、といった事項だけでなく、各分割ファイルごとに暗号化を行うか否かといった事項や、分割処理後に個々の分割ファイルに対して暗号化を行うのか、あるいは、暗号化を行った後にこれを複数のファイルに分割するのか、といった分割・暗号化の順番といった事項までも含ませておいてかまわない。

ステップＳ１９では、保管対象データを分割したり、分割した後に暗号化したり、または暗号化した後に分割したりする際に、いずれかの段階において、一定の規則に従って、保管対象データとは無関係なダミーデータを付加する方法が決定される。前述したように、保管時に、このようなダミーデータの付加処理を行っておけば、万一、保管されていたデータを盗み見られたり、これを復号化されたとしても、ダミーデータが介在しているために完全な復元には至らないので、セキュリティが更に向上することになる。

一方、ステップＳ２１で決定する事項は、既に述べたように、冗長格納方法としてミラーリング方式とパリティファイル作成方式とのいずれを選択するか、という事項でよい。

こうして、データ保管手順を実行するにあたって必要な事項が決定されたら、ステップＳ２３において、分割・暗号化手段１３が呼び出され、これまでの各ステップで決定された方法にしたがって、保管対象データファイルＦ１に対する分割処理、暗号化処理、ダミーデータの付加処理が行われ、複数の分割ファイルが作成される。なお、冗長格納方法としてパリティファイル作成方式が選択されていた場合には、この段階で、必要なパリティファイルの作成も行われる。続いて、個々の分割ファイル（本明細書では、パリティファイルも分割ファイルの１つとして取扱う）について、保管先となるデータサーバを決定し、これを書込む処理が行われる。すなわち、まず、ステップＳ２９において、１つの分割ファイルの保管先となるデータサーバが決定され、ステップＳ３１において、ネットワーク通信手段１６の動作により、この１つの分割ファイルが保管先となるデータサ

ーバへと転送され、当該データサーバ内に書込まれる。このような処理が、ステップＳ３５を経ることによって、全ての分割ファイルについて完了するまで、繰り返し実行される。このとき、ミラーリング方式で冗長格納する場合は、個々の分割ファイルが正、副の異なる２箇所のデータサーバに転送され、それぞれ格納されることになる。また、パリティファイル作成方式で冗長格納する場合は、各分割ファイルとともにパリティファイルも、所定のデータサーバに転送され、それぞれ格納されることになる。

ネットワーク通信手段１６によるこのようなファイル転送処理は、前述したように、ＦＴＰに則って実行される。具体的には、たとえば、保管先となるデータサーバのＵＲＬのリストを記録した設定ファイルを用意し、この設定ファイルのＵＲＬリストに記述されているデータサーバの１つを適当に選択して、１つの分割ファイルを転送し、うまく転送できたら、次の分割ファイルを、ＵＲＬリストに掲載されている次のデータサーバに対して転送するようにすればよい。転送が何らかの理由で失敗した場合は、転送先をＵＲＬリストの次のデータサーバに変更して、分割ファイルの転送をやり直すようにする。

最後に、ステップＳ３７において、データ管理手段１５の機能により、保管対象ファイルＦ１についての管理データが作成され、アーカイブカード１０内に記録される。具体的には、図２に示されているような各項目からなるデータ保管手順情報と、個々の分割ファイルの保管先となったデータサーバのＵＲＬリストからなるデータ保管場所情報と、によって構成される「ファイルＦ１の管理データ」が、Ｆ１用フォルダ内に記録される。以上で、保管対象ファイルとして指定されたファイルＦ１についての保管処理は完了し、再び、ステップＳ５の手順へと戻り、次のイベント待ちの状態になる。

続いて、ステップＳ７で発生するイベントとして、利用者が特定のファイルを指定して取出処理を選択した場合を考える。この場合、まず、ステップＳ４１において、データ管理手段１５の機能により、取出対象ファイルの管理データがアーカイブカード１０から読込まれる。たとえば、利用者が、既に保管済みのファイルＦ１を指定して、取出処理を選択した場合であれば、図２に示されている「ファイルＦ１の管理データ」がアーカイブカード１０から読み込まれる。この管

理データ内のデータ保管場所情報を参照すれば、取出対象ファイルを構成する個々の分割ファイルが保管されているデータサーバのＵＲＬを認識することができ、データ保管手順情報を参照すれば、保管時にどのような分割処理、暗号化処理、冗長格納処理、ダミーデータ付加処理が実行されたかを認識することができる。

そこで、ステップＳ４３では、データ保管場所情報に基づいて、ネットワーク通信手段１６を機能させることにより、取出対象ファイルＦ１を構成する個々の分割ファイルの読込み処理が実行され、所定のデータサーバに格納されていた個々の分割ファイル（必要に応じて、パリティファイル）が、分散型データアーカイブ装置１内に読み込まれる。更に、ステップＳ４７では、復号化・統合手段１４を機能させることにより、読込まれた個々の分割ファイルに対する復号化および統合処理がデータ保管手順情報に基づいて実行され、もとのファイルＦ１が復元される。もちろん、保管時に冗長格納処理が実行されていた場合には、特定のデータサーバに支障が生じていても、所定の復元手続きを行うことによりファイルの復元が可能になる。また、データの保管時に、ダミーデータを付加していた場合には、ステップＳ４７の処理を行う段階で、これを除去する。

最後に、こうして復元された取出対象ファイルＦ１を、利用者が指定した所定の記録場所（分散型データアーカイブ装置１として機能しているソフトウエアの管理外の指定場所）に保存する処理が行われる。このようにして、保管されていたデータは、再び利用者の手元に復元されることになる。上述した一連のデータ復元処理に必要な情報は、アーカイブカード１０内に管理データとして記録されており、分散型データアーカイブ装置１が、この管理データに基づいて自動的に復元処理を行うため、利用者は、対象となるデータファイルが複数の分割ファイルとして保管されていたことすら意識する必要は無い。

なお、ステップＳ７のイベントとして、利用者がメニューから終了を選択した場合は、ステップＳ５３へと進み、これまでに復元したファイルが分散型データアーカイブ装置１内（分散型データアーカイブ装置１として機能しているソフトウエアの管理下の場所）に残っていた場合には、これを消去する処理を行った上で、分散型データアーカイブ装置１としての動作を終了する（分散型データアー

カイブ装置１として機能しているソフトウエアの実行を終了する）。また、ステップＳ７のイベントとして、利用者がアーカイブカード１０を読取・書込手段１１から排出する指示を与えた場合は、ステップＳ３においてカードが排出された後、ステップＳ１に戻り、次のカードの挿入待ちの状態となる。

以上説明したとおり、本発明によれば、貴重なデジタルデータを分割し、複数のデータサーバに保管するので、保管したデータを１個所のサーバから盗んでも元のデータに復元できないので安全である。データの保管処理や、データの取出処理を行うには、アーカイブカード１０が必要になり、このアーカイブカード１０としては、不正なデータ改竄が極めて困難なＩＣカードを用いることができるので、ＩＣカードを盗まれない限り、保管したデータを盗まれる心配はない。また、保管対象データは必要に応じて暗号化して保管できるので、インターネット上のデータサーバからデータを取り出す時に万一盗聴されても、大きな問題は生じない。しかも、保管先のデータサーバは、インターネットの標準プロトコルであるＦＴＰで接続できれば十分であり、他には特別な仕掛けは一切不要なので、保管先をかなり自由に選択できる。アーカイブカード１０を携帯していれば、ネットワークに接続された任意の分散データアーカイブ装置から、保管データにアクセスが可能であり、たいへん便利である。もちろん、ネットワークを介してデータサーバとの間でファイルを転送するプロトコルは、ＦＴＰに限定されるわけではなく、この他にも種々のプロトコルを利用することが可能である。

§３．種々の変形例および応用例

続いて、本発明の変形例および応用例を述べる。まず、図１に示す実施形態では、分散型データアーカイブ装置１と、データサーバ２（２ａ，２ｂ，２ｃ）とを全く別の機能をもった装置として説明したが、いずれも「所定のソフトウエアを組み込んだコンピュータ」という点では同じであり、実際には、全く同一のハードウエア構成をもったコンピュータを、一方では分散型データアーカイブ装置１として用い、他方ではデータサーバ２として用いる、というような利用形態も可能である。ハードウエア的には同一のコンピュータであっても、組み込むべきソフトウエアによって、分散型データアーカイブ装置１として用いることもできるし、データサーバ２として用いることもできる。もちろん、両方のソフトウエ

アを組み込んだコンピュータであれば、あるときには分散型データアーカイブ装置１として機能させ、別なときにはデータサーバ２として機能させる、という使い分けも可能である。

たとえば、３つの支社Ｘ，Ｙ，Ｚにそれぞれコンピュータが設置されており、これらのコンピュータが互いにネットワークで接続されていた場合に、これら各コンピュータのそれぞれに、分散型データアーカイブ装置１として機能させるためのソフトウエアと、データサーバ２として機能させるためのソフトウエアと、を組み込んでおけば、１つの支社のデータを２つに分割し（たとえば、奇数番目のバイトからなる第１の分割ファイルと、偶数番目のバイトからなる第２の分割ファイルと、を作成すればよい）、他の２社のコンピュータに保管してバックアップする、というような利用形態も可能である。具体的には、支社Ｘのデータのバックアップを、支社Ｙおよび支社Ｚのコンピュータに保管する際には、支社Ｘのコンピュータをデータアーカイブ装置１として機能させ、支社Ｙおよび支社Ｚのコンピュータをデータサーバ２として機能させればよい。同様に、支社Ｙのデータのバックアップを、支社Ｘおよび支社Ｚのコンピュータに保管する際には、支社Ｙのコンピュータをデータアーカイブ装置１として機能させ、支社Ｘおよび支社Ｚのコンピュータをデータサーバ２として機能させればよいし、支社Ｚのデータのバックアップを、支社Ｘおよび支社Ｙのコンピュータに保管する際には、支社Ｚのコンピュータをデータアーカイブ装置１として機能させ、支社Ｘおよび支社Ｙのコンピュータをデータサーバ２として機能させればよい。このように、本発明における「データアーカイブ装置１」あるいは「データサーバ２」なる構成要素の名称は、ある１つのファイルを保管したり、取出したりする作業を行うときの役割を示しているにすぎず、実際には、ネットワーク上に接続されている個々のコンピュータを、「データアーカイブ装置１」として機能させることもできるし、「データサーバ２」として機能させることもできる。

また、上述の実施形態では、図２に示すような管理データを、アーカイブカード１０（携帯可能記録媒体）に直接記録するようにしているが、管理データは、必ずしもアーカイブカード１０に直接記録する必要はない。たとえば、図１に示すブロック図におけるデータサーバ２ａ内に、図２に示す管理フォルダ全体を置

くようにし、アーカイブカード１０には、この管理フォルダをアクセスするために必要な情報（たとえば、データサーバ２ａのＵＲＬを示す情報や管理データが格納されたアドレスを示す情報とか、管理フォルダをアクセスするために必要なパスワードの情報など）を記録しておくような方式を採ることも可能である。このような方式を採る場合、データの保管処理を行う際には、データ管理手段１５は、作成した管理データをアーカイブカード１０内に直接記録する代わりに、データサーバ２ａ内の所定アドレス場所に書込む処理を行い、アーカイブカード１０内には、「データサーバ２ａ内に書込まれた管理データをアクセスするために必要な情報」を記録する処理を行うようにすればよい。また、データの取出処理を行う際には、データ管理手段１５は、必要な管理データをアーカイブカード１０から直接読み込む代わりに、まず、アーカイブカード１０に記録されている「データサーバ２ａ内に書込まれた管理データをアクセスするために必要な情報」を読み出し、この情報を利用して、データサーバ２ａから管理データを読み出す処理を行うようにすればよい。この方式は、いわば、管理データをアーカイブカード１０に間接的に記録する方式ということができる。

このように、管理データをアーカイブカード１０に間接的に記録する方式を採ると、次のような２つのメリットが得られる。第１のメリットは、アーカイブカード１０（携帯可能記録媒体）の記録容量の制限を緩和することができるというメリットである。図２に示す例のように、各ファイルの管理データは、データ保管手順情報とデータ保管場所情報とによって構成されており、全体としてある程度のデータ量を有している。一方、アーカイブカード１０は、カード状の電子情報記録媒体であるため、その記録容量は比較的少ない。したがって、多数のファイルについての管理データを、アーカイブカード１０内に直接記録することは、限られた記録容量を浪費する点で好ましくない。管理データをアーカイブカード１０に間接的に記録する方式を採れば、管理データは実際にはアーカイブカード１０以外の記録場所に格納されることになり、アーカイブカード１０内には、この管理データをアクセスするために必要な情報だけを記録しておけばよいので、限られた記録容量を有効利用することができる。

管理データをアーカイブカード１０に間接的に記録する方式のもうひとつのメ

リットは、保管されているデータを、複数の利用者によって共用させるような運用形態が可能になる点である。たとえば、同一グループに所属する数名の利用者に対して、同種のアーカイブカード１０を配付しておき、この同種のアーカイブカード１０内には、特定の記録場所に格納されている同一の管理データをアクセスするために必要な情報を記録しておくようにする。そうすれば、この同種のアーカイブカード１０を所持している利用者なら誰でも、同一の管理データにアクセスすることが可能になり、この同一の管理データに基づいて、保管されている同一のデータを取出すことができる。

また、本発明に係るデータアーカイブシステムでは、保管対象データに期間に関する制限を示す期間制限情報を付加した上で、これをデータサーバに分散して保管させるようにし、取出処理を行う際には、この期間制限情報に基づく制限を課することも可能である。具体的には、たとえば、図４に示す例のように、各分割ファイルＦ１１，Ｆ１２，Ｆ１３のそれぞれに、所定のフォーマットで期間制限情報を付加して、各データサーバに保管する処理を行えばよい。たとえば、「２００１年６月末日まで取出禁止」というような期間制限情報が付加されている分割ファイルに対しては、利用者から取出指示があったとしても、その指示が取出禁止期間中に与えられた場合であれば、取出しが制限されるような運用を行うことが可能である。このような期間制限に関するチェックは、各データサーバ２側で行うことも可能であるし、分散型データアーカイブ装置１側で行うことも可能であり、アーカイブカード１０内で行うことも可能である。また、期間制限情報としては、「２００１年７月以降は取出禁止」というような制限を設定することも可能であるし、「２００１年７月～９月までの期間は取出禁止」というような制限を設定することも可能である。あるいは、「２００１年７月１日になったら、本データを削除せよ」というような能動的な指示を設定し、データサーバ側で期限がきたら自動的に削除させるような運用も可能である。

また、本発明に係るデータアーカイブシステムでは、各データサーバに分散して保管される個々の分割ファイルに、本来の保管先とは異なる退避先を示す退避先情報を付加するとともに、この退避先情報を管理データの一部として記録しておくようにし、本来の保管先となるデータサーバに何らかの支障が生じた場合に

は、保管されているデータを、退避先として指定された別なデータサーバに退避させる処理を行うことも可能である。

たとえば、保管対象ファイルＦ１が、３つの分割ファイルＦ１１，Ｆ１２，Ｆ１３に分割され、これら各分割ファイルが、それぞれデータサーバ２ａ，２ｂ，２ｃに保管されることになったとしよう。この場合、各分割ファイルＦ１１，Ｆ１２，Ｆ１３の本来の保管先は、それぞれデータサーバ２ａ，２ｂ，２ｃということになり、実際、各分割ファイルＦ１１，Ｆ１２，Ｆ１３は、ＦＴＰによってそれぞれデータサーバ２ａ，２ｂ，２ｃへと転送され、書込まれることになる。退避先情報は、この転送時に各分割ファイルＦ１１，Ｆ１２，Ｆ１３に付加されることになる。たとえば、分割ファイルＦ１１およびＦ１２についての退避先を第４のデータサーバ２ｄとし、分割ファイルＦ１３についての退避先を第５のデータサーバ２ｅとするのであれば、図５に示す例のように、各分割ファイルＦ１１，Ｆ１２，Ｆ１３には、それぞれＵＲＬ（２ｄ），ＵＲＬ（２ｄ），ＵＲＬ（２ｅ）なる退避先情報を付加するようにすればよい（ここで、ＵＲＬ（ｘｘ）は、データサーバｘｘのＵＲＬを示す情報を示している。）。

一方、保管対象ファイルＦ１の管理データにも、各分割ファイルに付加した退避先情報を付加しておくようにする。具体的には、図６に示すようなデータ保管場所情報（データサーバのＵＲＬリスト）を作成し、これをアーカイブカード１０などに管理データとして記録するようにする。この図６に示す例では、各分割ファイルＦ１１，Ｆ１２，Ｆ１３の本来の保管先を示す情報は、それぞれＵＲＬ（２ａ），ＵＲＬ（２ｂ），ＵＲＬ（２ｃ）となっており、通常の処理手順によれば、各分割ファイルＦ１１，Ｆ１２，Ｆ１３は、それぞれデータサーバ２ａ，２ｂ，２ｃに保管されることになる。ただし、各分割ファイルＦ１１，Ｆ１２，Ｆ１３の退避先として、ＵＲＬ（２ｄ），ＵＲＬ（２ｄ），ＵＲＬ（２ｅ）なる情報が記録されており、退避先となるデータサーバが、それぞれデータサーバ２ｄ，２ｄ，２ｅであることが示されている。

ここで、第１のデータサーバ２ａをこのまま運用することに何らかの支障が生じた場合を考えよう。たとえば、データサーバ２ａの情報容量がほぼ満杯になり、現在蓄積されているデータの一部を他のデータサーバに移さなければ、重大な

トラブルの発生が懸念されるとか、あるいは、データサーバ２ａを構成するハードディスクの保守点検を行うために、現在蓄積されているデータを一時的に他のデータサーバに移す必要がある、というような事情が生じたものとしよう。このような場合、第１のデータサーバ２ａに保管されている分割ファイルＦ１１には、図５に示すように、ＵＲＬ（２ｄ）なる退避先情報が付加されているので、第１のデータサーバ２ａは、この退避先情報にしたがって、分割ファイルＦ１１を退避先となる第４のデータサーバ２ｄへと転送する処理を行うことができる。

このような退避のための転送処理が行われた後に、ファイルＦ１に対する取出処理が実行されると、分散型データアーカイブ装置１は、図６に示すデータ保管場所情報の保管先の欄に記載されている本来のデータサーバから、必要な分割ファイルＦ１１，Ｆ１２，Ｆ１３を読み出す処理を試みる。すると、データサーバ２ｂからは分割ファイルＦ１２が読み出され、データサーバ２ｃからは分割ファイルＦ１３が読み出されるが、データサーバ２ａから分割ファイルＦ１１を読み出す試みは失敗に終わる。このように、本来の保管先からの読み出しが失敗した場合には、退避先からの読み出しが試みられる。この例の場合、分割ファイルＦ１１に関しては、図６に示すデータ保管場所情報の退避先の欄に記載されているデータサーバ２ｄから、分割ファイルＦ１１を読み出す処理が試みられることになる。かくして、別なデータサーバへの退避が行われたにもかかわらず、分割ファイルＦ１１は正常に読み出されることになる。

もちろん、退避させるべき原因がなくなったら、分割ファイルＦ１１を元通り本来の保管先であるデータサーバ２ａへ戻す処理を行えばよい。このように、退避先情報を付加しておくようにすれば、万一、データを別なデータサーバへ退避させねばならない事情が生じたとしても、データの取出処理は支障なく実行されることになる。

なお、退避先となるデータサーバは、データファイルを保管する処理を行うときに、利用者自身が指定することもできるが、実用上は、分散型データアーカイブ装置１によって自動的に退避先を決定する処理が行われるようにするのが好ましい。あるいは、データサーバ側から、分散型データアーカイブ装置１に対して、退避先とすべき別なデータサーバを指定する処理を行ってもよい。

産業上の利用可能性

本発明に係るデータアーカイブ装置およびデータアーカイブシステムは、任意のデジタルデータの保管に広く利用することができ、特に、インターネットなどの広域ネットワークを利用して、貴重なデジタルデータをバックアップする用途に最適である。

【図面の簡単な説明】

図１は、本発明の一実施形態である分散型データアーカイブシステムの全体構成図である。

図２は、携帯可能記録媒体１０の中に記録されている管理データの一例を示す図である。

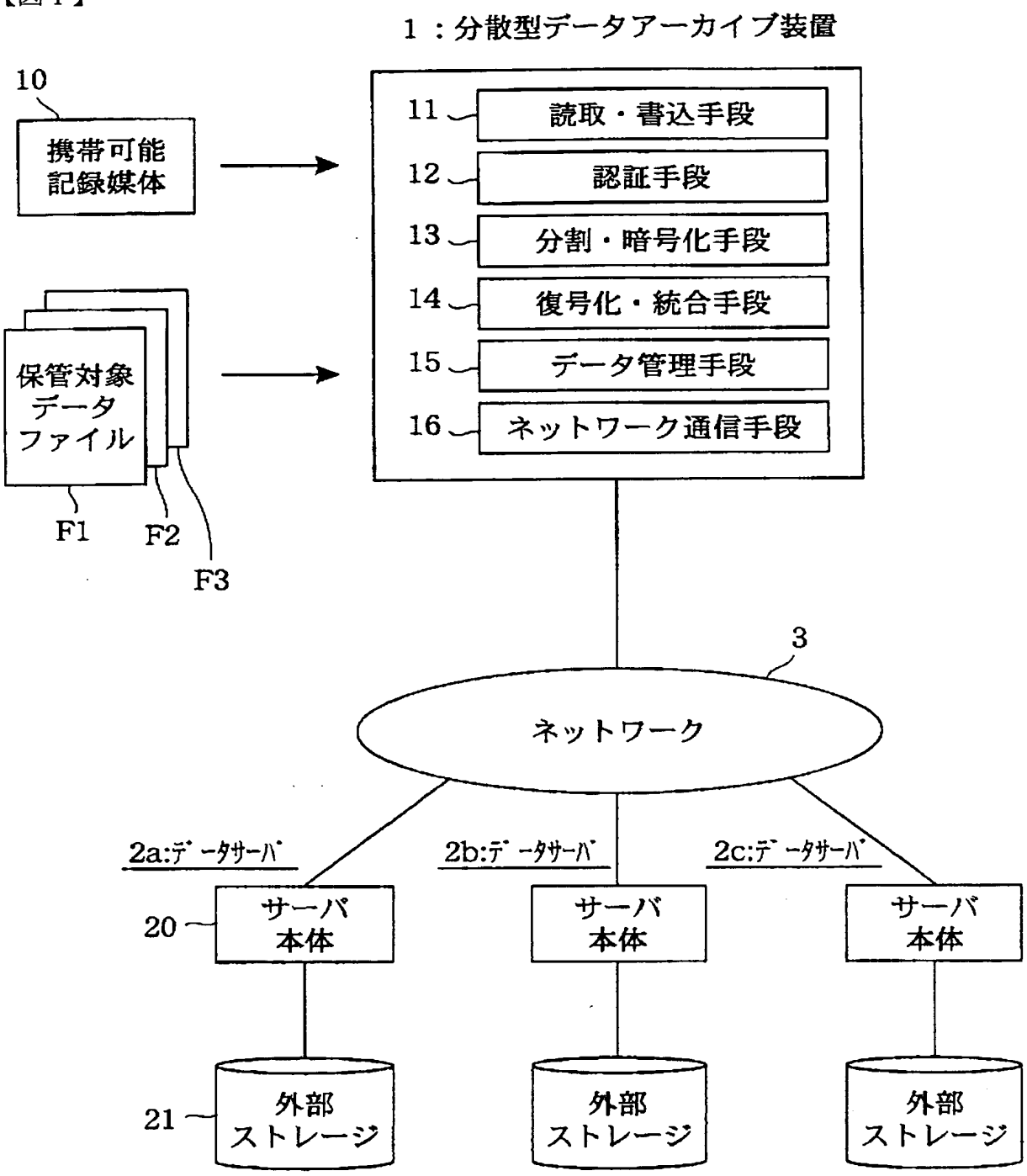
図３は、分散型データアーカイブ装置１の動作の流れを示す流れ図である。

図４は、データサーバに保管される各分割ファイルに、期間制限情報を付加した例を示す図である。

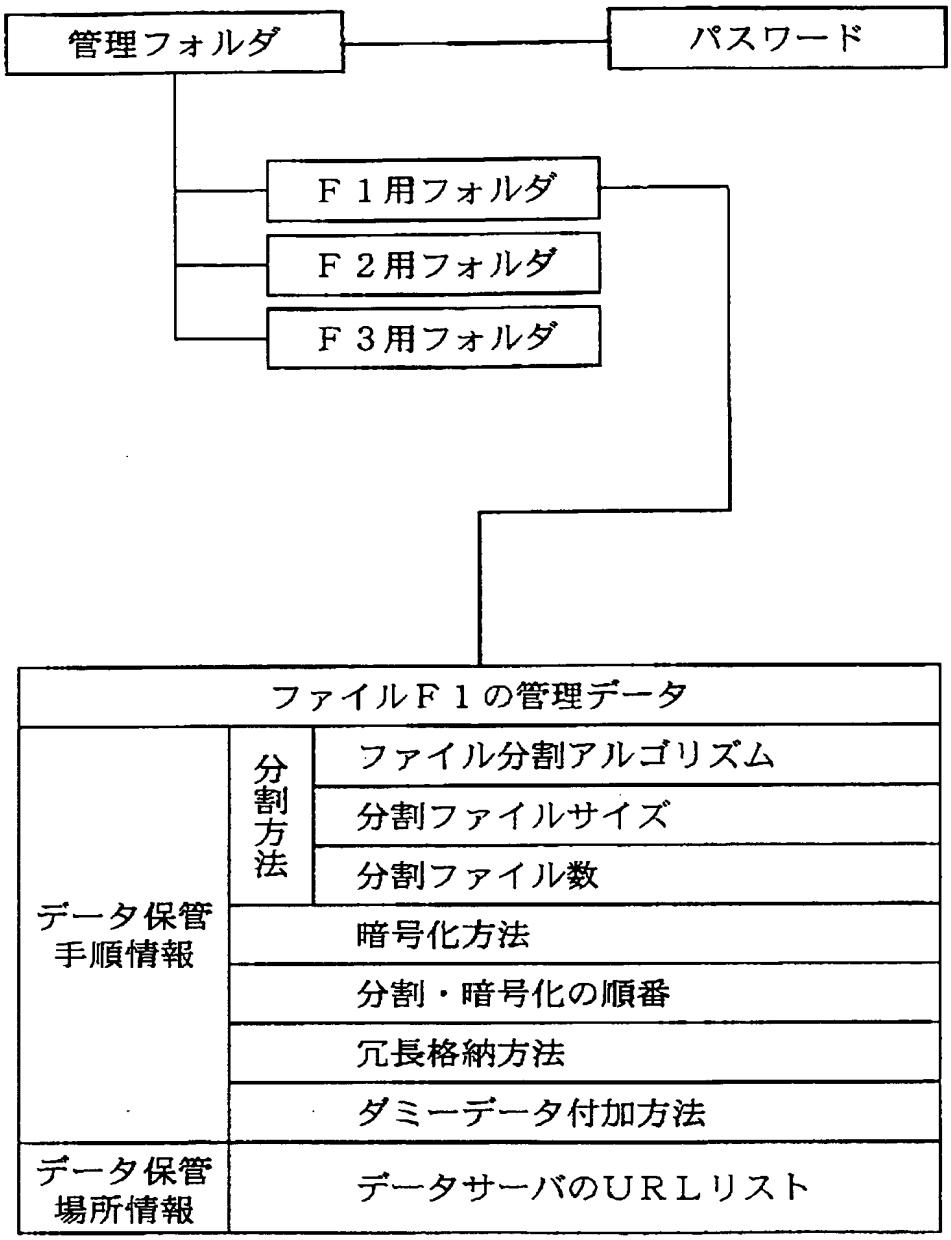
図５は、データサーバに保管される各分割ファイルに、退避先情報を付加した例を示す図である。

図６は、図５に示す退避先情報をもった管理データの一例を示す図である。

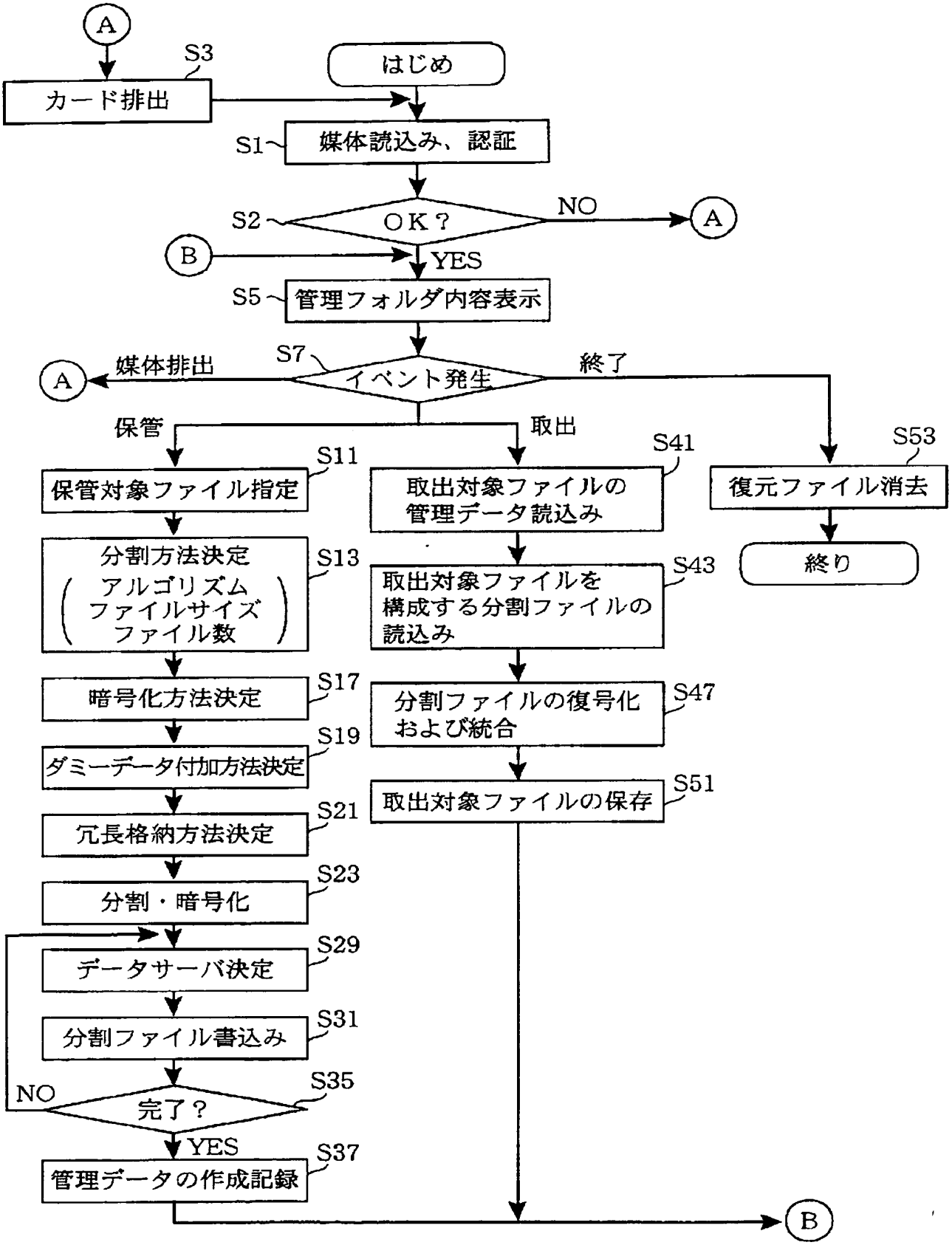
【図１】


１：分散型データアーカイブ装置
10
携帯可能
記録媒体
保管対象
データ
ファイル
F1
F2
F3
11
読取・書込手段
12
認証手段
13
分割・暗号化手段
14
復号化・統合手段
15
データ管理手段
16
ネットワーク通信手段
3
ネットワーク
2a:ﾃﾞｰﾀｻｰﾊﾞ
2b:ﾃﾞｰﾀｻｰﾊﾞ
2c:ﾃﾞｰﾀｻｰﾊﾞ
20
サーバ
本体
サーバ
本体
サーバ
本体
21
外部
ストレージ
外部
ストレージ
外部
ストレージ

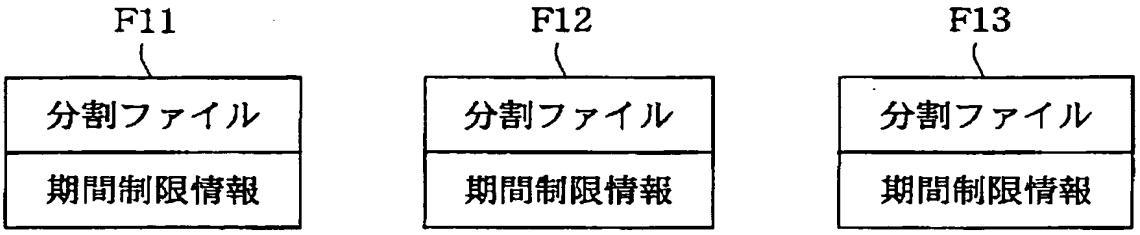
【図２】


管理フォルダ
パスワード
Ｆ１用フォルダ
Ｆ２用フォルダ
Ｆ３用フォルダ
ファイルＦ１の管理データ
データ保管手順情報
分割方法
ファイル分割アルゴリズム
分割ファイルサイズ
分割ファイル数
暗号化方法
分割・暗号化の順番
冗長格納方法
ダミーデータ付加方法
データ保管場所情報
データサーバのＵＲＬリスト

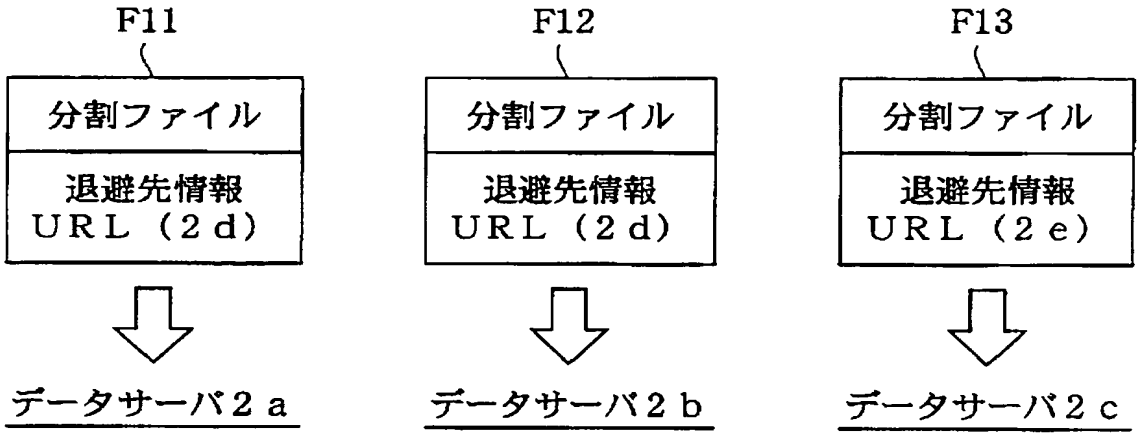
【図３】


A
S3
カード排出
はじめ
S1
媒体読込み、認証
S2
OK？
NO
A
B
YES
S5
管理フォルダ内容表示
S7
媒体排出
イベント発生
終了
保管
取出
S11
保管対象ファイル指定
S41
取出対象ファイルの
管理データ読込み
S53
復元ファイル消去
分割方法決定
（アルゴリズム
ファイルサイズ
ファイル数）
S13
S43
取出対象ファイルを
構成する分割ファイルの
読込み
終り
暗号化方法決定
S17
S47
分割ファイルの復号化
および統合
ダミーデータ付加方法決定
S19
S51
取出対象ファイルの保存
冗長格納方法決定
S21
分割・暗号化
S23
データサーバ決定
S29
分割ファイル書込み
S31
NO
完了？
S35
YES
管理データの作成記録
S37
B

【図４】



【図５】



【図６】

データ保管場所情報

分割ファイル	保管先	退避先
Ｆ１１	URL（２ａ）	URL（２ｄ）
Ｆ１２	URL（２ｂ）	URL（２ｄ）
Ｆ１３	URL（２ｃ）	URL（２ｅ）

【手続補正書】

【提出日】平成１３年８月３０日（２００１．８．３０）

【手続補正１】

【補正対象書類名】明細書

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【発明の名称】　分散型データアーカイブ装置およびシステム

【特許請求の範囲】

【請求項１】 ネットワーク（３）を介してアクセス可能な複数のデータサーバ（２ａ，２ｂ，２ｃ）に、保管対象データ（Ｆ１）を分散して保管する機能と、保管されていたデータを必要に応じて取出す機能と、を有する分散型データアーカイブ装置（１）であって、

データ保管時に、保管対象データ（Ｆ１）を所定の分割方法に基づいて複数の分割ファイル（Ｆ１１，Ｆ１２，Ｆ１３）に分割する分割手段（１３）と、

データ取出時に、前記分割方法を考慮して前記複数の分割ファイルを統合して元の保管対象データに復元する統合手段（１４）と、

データ保管時には、前記複数の分割ファイルを、前記ネットワークを介してそれぞれ所定のデータサーバへ転送して保管させる処理を行い、データ取出時には、前記ネットワークを介して個々のデータサーバに保管されている前記複数の分割ファイルを取出す処理を行うネットワーク通信手段（１６）と、

データ保管時には、前記分割手段によって採られた分割方法を示す情報を含んだデータ保管時の手順を示すデータ保管手順情報と、前記ネットワーク通信手段によって転送された複数の分割ファイルの保管先となるデータサーバを特定するデータ保管場所情報と、を有する管理データを作成し、この管理データを所定の場所に記録する処理を行い、データ取出時には、前記管理データを読み出し、この管理データに含まれている前記データ保管手順情報を前記統合手段に与え、この管理データに含まれている前記データ保管場所情報を前記ネットワーク通信手段に与える処理を行うデータ管理手段（１５）と、

を備えることを特徴とする分散型データアーカイブ装置。

【請求項２】　請求項１に記載の分散型データアーカイブ装置において、

携帯可能記録媒体（１０）に対して、データの読み書きを行う機能をもった読取・書込手段（１１）を更に備え、データ管理手段（１５）が、前記読取・書込手段を介して前記携帯可能記録媒体内に管理データを記録する処理を行うことを特徴とする分散型データアーカイブ装置。

【請求項３】　請求項１に記載の分散型データアーカイブ装置において、

所定の場所に記録されている管理データをアクセスするために必要なアクセス情報が格納された携帯可能記録媒体（１０）に対して、データの読み書きを行う機能をもった読取・書込手段（１１）を更に備え、データ管理手段（１５）が、前記読取・書込手段を介して前記携帯可能記録媒体内の前記アクセス情報を読み出し、このアクセス情報に基づいて管理データへのアクセスを行うことを特徴とする分散型データアーカイブ装置。

【請求項４】　請求項１～３のいずれかに記載の分散型データアーカイブ装置において、

利用者の正当性を検査する認証手段（１２）を更に備え、正しい認証結果が得られた場合にのみ、データ保管処理もしくはデータ取出処理が実行されるようにしたことを特徴とする分散型データアーカイブ装置。

【請求項５】　請求項１～４のいずれかに記載の分散型データアーカイブ装置において、

分割手段が、保管対象データを分割する処理を行うプロセスにおいて、データに対する暗号化処理を行う分割・暗号化手段（１３）として機能し、

データ管理手段（１５）が、前記暗号化処理の方法を示す情報を含んだデータ保管手順情報を作成して、これを管理データとして記録する機能を果たし、

統合手段が、分割ファイルを統合して元の保管対象データに復元する際に、前記データ保管手順情報に含まれている前記暗号化処理の方法を示す情報に基づいて、暗号化された部分に対する復号化処理を行う復号化・統合手段（１４）として機能するようにしたことを特徴とする分散型データアーカイブ装置。

【請求項６】　請求項５に記載の分散型データアーカイブ装置において、

データ管理手段（１５）が、暗号化処理の方法を示す情報の一部として、分割処理と暗号化処理とについての実行順を示す情報を用いることを特徴とする分散型データアーカイブ装置。

【請求項７】 請求項１～６のいずれかに記載の分散型データアーカイブ装置において、

分割手段（１３）が、保管対象データを分割する処理を行うプロセスにおいて、前記保管対象データとは無関係なダミーデータを付加する処理を行うようにし、

データ管理手段（１５）が、ダミーデータ付加処理に関する情報を含んだデータ保管手順情報を作成して、これを管理データとして記録する機能を果たし、

統合手段（１４）が、分割ファイルを統合して元の保管対象データに復元する際に、前記データ保管手順情報に含まれている前記ダミーデータ付加処理に関する情報に基づいて、付加されていたダミーデータの除去処理を行うようにしたことを特徴とする分散型データアーカイブ装置。

【請求項８】 請求項１～７のいずれかに記載の分散型データアーカイブ装置において、

分割手段（１３）が、保管対象データを分割して複数の分割ファイルを作成する処理を行うプロセスにおいて、前記保管対象データに冗長度を付加して保管するために必要な冗長格納処理を行うようにし、

データ管理手段（１５）が、前記冗長格納処理に関する情報を含んだデータ保管手順情報を作成して、これを管理データとして記録する機能を果たし、

統合手段（１４）が、前記データ保管手順情報に含まれている前記冗長格納処理に関する情報を考慮して、元の保管対象データを復元する処理を行うようにしたことを特徴とする分散型データアーカイブ装置。

【請求項９】 請求項１～８のいずれかに記載の分散型データアーカイブ装置において、

データ保管時に、期間に関する制限を示す期間制限情報を、保管対象データに付加した上で、データサーバに分散して保管する機能を更に設け、

データ取出時に、前記期間制限情報に基づく制限を考慮した取出処理が行われ

るようにしたことを特徴とする分散型データアーカイブ装置。

【請求項１０】 請求項１～９のいずれかに記載の分散型データアーカイブ装置において、

データ保管時に、各データサーバに分散して保管される個々の分割ファイルに、本来の保管先とは異なる退避先を示す退避先情報を付加するとともに、この退避先情報を管理データの一部として記録する機能を更に設け、

データ取出時に、本来の保管先となるデータサーバから所望の分割ファイルを取出すことができない場合には、前記退避先情報によって示された退避先となるデータサーバから前記所望の分割ファイルを取出す処理が行われるようにしたことを特徴とする分散型データアーカイブ装置。

【請求項１１】 請求項１～１０のいずれかに記載の分散型データアーカイブ装置（１）と、この分散型データアーカイブ装置が接続されたネットワーク（３）と、このネットワーク（３）を介して前記分散型データアーカイブ装置からのアクセスを受ける複数のデータサーバ（２ａ，２ｂ，２ｃ）と、「前記分散型データアーカイブ装置内で作成された管理データ」もしくは「この管理データをアクセスするために必要な情報」の記録場所として利用される携帯可能記録媒体（１０）と、を備えることを特徴とする分散型データアーカイブシステム。

【請求項１２】 請求項１１に記載の分散型データアーカイブシステムにおいて、

ネットワークに接続された端末装置が、分散型データアーカイブ装置（１）としての機能とデータサーバ（２ａ，２ｂ，２ｃ）としての機能とを兼ね備えるようにし、用途に応じてこれら２つの機能を選択可能な構成としたことを特徴とする分散型データアーカイブシステム。

【請求項１３】 請求項１１または１２に記載の分散型データアーカイブシステムにおいて、

携帯可能記録媒体（１０）としてＩＣカードを用い、分散型データアーカイブ装置（１）が前記携帯可能記録媒体にアクセスを行う際には、当該携帯可能記録媒体自体の正当性検査を行うようにしたことを特徴とする分散型データアーカイブシステム。

【請求項１４】 請求項１１～１３のいずれかに記載の分散型データアーカイブシステムにおいて、

複数の携帯可能記録媒体（１０）に、同一の管理データをアクセスするために必要な情報が格納されていることを特徴とする分散型データアーカイブシステム。

【請求項１５】 請求項１１～１４のいずれかに記載の分散型データアーカイブシステムにおいて、

分散型データアーカイブ装置（１）が、データ保管時に、各データサーバ（２ａ，２ｂ，２ｃ）に分散して保管される個々の分割ファイルに、本来の保管先とは異なる退避先を示す退避先情報を付加する機能を有し、

データサーバ（２ａ，２ｂ，２ｃ）が、分割ファイルの保管を継続することに支障が生じた場合に、保管中の分割ファイルを前記退避先情報によって示されている退避先となる別なデータサーバに退避させる処理を行う機能を有することを特徴とする分散型データアーカイブシステム。

【請求項１６】 請求項１～１０のいずれかに記載の分散型データアーカイブ装置を実現するプログラムを記録したコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタルデータを、ネットワークを利用して所定の場所に保管し、必要なときにこれを取り出すことが可能なデータアーカイブ装置およびデータアーカイブシステムに関する。特に、本発明は、バックアップの目的で、貴重なデジタルデータの複製を、ネットワーク上の複数の箇所に分散して保管することができるデータアーカイブシステムに関する。

【０００２】

【従来の技術】

データを作成したコンピュータ等から、ネットワークで接続されている他のファイルサーバ等に、作成したデータのバックアップデータを転送し、貴重なデータの保管を行うことは広く行われている。このネットワークを、たとえば、イン

ターネットのような世界的規模の広域ネットワークにまで拡張すれば、インターネットにアクセスすることができる環境さえあれば、世界中のどこからでもデータの保管を行うことができ、保管されていたデータを世界中のどこからでも取り出すことができる。

【０００３】

【発明が解決しようとする課題】

しかしながら、利用するネットワークの規模を拡大すればするほど、利用者の利便性は向上するが、逆にセキュリティは低下することになる。保管対象となるデータは、通常、個人個人のプライベートな情報を含んでおり、データを預けた本人あるいは本人の委託を受けた代理人だけが取り出せるよう、十分なセキュリティを確保しておく必要がある。このように、ネットワークを利用した従来のデータアーカイブシステムには、どこからでもデータの預け入れや取り出しができるように利便性を向上させると、セキュリティが低下するという問題が生じていた。

【０００４】

本発明はこのような問題を考慮してなされたものであり、データを預けた本人あるいはデータへのアクセスを許可された特定の者だけが、任意の場所から預け入れたデータに安全にアクセスでき、しかもデータを保管するサーバ側に特別な装置やソフトウエアの用意を必要としないデータアーカイブシステムを提供することを目的とする。

【０００５】

【課題を解決するための手段】

上記課題を解決するために、本発明は、利用者の正当性検査を行う認証手段と、保管対象データを複数の部分に分割する分割手段と、分割保管されたデータを元の単一データファイルに復元する統合復元手段と、保管対象データを納めたデータサーバとの間で定められた通信プロトコルにより、分割されたデータファイルを転送するネットワーク通信手段と、新規にデータ保管を行う時に、保管対象データの保管場所を示すデータ保管場所情報および保管対象データの分割方法等を示すデータ保管手順情報を記録するデータ管理手段と、を備えた分散型データ

アーカイブ装置を用意し、保管対象データを保管する際には、これを複数の部分に分割し、分割された個々の部分毎にネットワーク上の複数のサーバに転送して分散保管させ、保管対象データを取り出す際には、保管時に記録されたデータ保管場所情報およびデータ保管手順情報にしたがって、ネットワーク上の複数のサーバに分散して保管されている保管対象データを取り出し、これを合成して元のファイルに復元して利用者に提供するようしたものである。データを分割して複数のサーバに保管すれば、貴重なデータの盗み出しは困難である。

【０００６】

また、上記課題を解決するために、本発明は、携帯可能記録媒体に対してデジタルデータの書込みおよび読み出しを行う機能をもった読取・書込手段と、利用者の正当性検査を行う認証手段と、保管対象データを複数の部分に分割する分割手段と、分割保管されたデータを元の単一データファイルに復元する統合復元手段と、保管対象データを納めたデータサーバとの間で定められた通信プロトコルにより、分割されたデータファイルを転送するネットワーク通信手段と、新規にデータ保管を行う時に、保管対象データの保管場所を示すデータ保管場所情報および保管対象データの分割方法等を示すデータ保管手順情報を、前記携帯可能記録媒体に記録するデータ管理手段と、を備えた分散型データアーカイブ装置を用意し、この分散型データアーカイブ装置と、前記携帯可能記録媒体と、ネットワークと、複数のデータサーバと、によって、分散型データアーカイブシステムを構成し、保管対象データを保管する際には、前記携帯可能記録媒体に記録したデータ保管場所情報およびデータ保管手順情報にしたがって、この保管対象データを複数の部分に分割し、分割された個々の部分毎にネットワーク上の複数のサーバに転送して分散保管させ、保管対象データを取り出す際には、前記携帯可能記録媒体に記録されたデータ保管場所情報およびデータ保管手順情報にしたがって、ネットワーク上の複数のサーバに分散して保管されている保管対象データを取り出し、これを合成して元のファイルに復元して利用者に提供するようしたものである。このシステムでは、前記携帯可能記録媒体を携帯していれば、ネットワークに接続された任意の分散型データアーカイブ装置から保管データにアクセスすることが可能となる。たとえば、利用者は、データ保管場所情報およびデータ

保管手順情報を記録した、フロッピーディスクのような記録媒体を携帯していれば、ネットワークに接続された任意の分散型データアーカイブ装置にログインすることにより、どこからでも所望のアーカイブデータを取り出すことができる。

【０００７】

更に、データを暗号化する手段を付加し、分割手段によって保管対象データを分割した後に暗号化するか、または保管対象データに暗号化を施した後に分割して、保管すべき複数の分割データを作成するようにし、データ管理手段によって、暗号化や復号化に必要な暗号鍵情報等をデータ保管手順情報として記録するようにし、統合復元手段は、記録されているデータ保管手順情報に従って、保管されていた個々の分割データを復号化してから統合化するか、または先に統合してから復号化するかして、元のデータに復元するようにすると、より強力な効果を奏する。個々の分割データを暗号化すれば、元のデータを知ることは困難であり、インターネットのようなオープンなネットワーク上でデータを保管しても、データを取り出す時に盗み見される心配は実質的に無い。

【０００８】

また、データの保管時に、保管対象データを分割したり、分割した後に暗号化したり、または暗号化して後に分割したりする際に、いずれかの段階において、一定の規則に従ってダミーデータを付加するようにし、データ管理手段によって、このダミーデータ付加規則をデータ保管手順情報として記録しておくようにし、データの取出時には、データ保管手順情報に従って、保管されていた分割データに対する統合化や復号化処理を行う際の所定の段階において、保管時に付加されたダミーデータを除去するようにすれば、保管されていたデータを盗み見されたり、これを復号化されたとしても、ダミーデータが介在しているために完全な復元には至らないので、保管されていたデータを盗まれた場合の安全性が更に高まる。

【０００９】

更に、分割したデータを冗長性を持たせて複数のデータサーバに保管しておくようにすれば、どれか１つのデータサーバがダウンしても、他の正常なサーバのデータだけから元のデータを復元できるようになる。データサーバ自体がダウン

することも考慮すると、このような分散型データアーカイブシステムはより安全である。

【００１０】

また、上述した携帯可能記録媒体としては、セキュリティの高いＩＣカードを用いることがより望ましい。こうすることにより、記録されているデータ保管場所情報やデータ保管手順情報の読み出し、コピーなどがより困難となり、ＩＣカード所有者だけが保管されているデータにアクセスできることになる。

【００１１】

また、上記分散型データアーカイブ装置は、汎用のコンピュータに、専用のプログラムを組み込むことにより実現することができ、そのような専用のプログラムは、コンピュータ読取り可能な記録媒体に記録して配付することができる。ネットワークを介してデータサーバに接続することができる任意の汎用コンピュータに、上記専用プログラムを組み込めば、当該汎用コンピュータを本発明に係る分散型データアーカイブ装置として利用することができるようになり、携帯可能記録媒体を携帯している限り、実質的に任意の場所から保管されたデータにアクセスすることができる。

【００１２】

【発明の実施の形態】

§１．基本的な実施形態

まず、本発明の基本的な実施形態を説明する。図１は、本発明に係る分散型データアーカイブシステムの全体構成図である。分散型データアーカイブ装置１は、この分散型データアーカイブシステムの中枢をなす装置であり、複数のデータサーバ２（図１では２ａ，２ｂ，２ｃ）に対して、ネットワーク３を介して、所望のデータを保管する機能を有している。この分散型データアーカイブ装置１には、携帯可能記録媒体１０を挿入することができ、上記機能を実行する際には、分散型データアーカイブ装置１と携帯可能記録媒体１０との連携動作が行われる。分散型データアーカイブ装置１は、図１に示されているように、読取・書込手段１１、認証手段１２、分割･暗号化手段１３、復号化･統合手段１４、データ管理手段１５、ネットワーク通信手段１６から構成される。これら各手段の個々の

機能については後述する。利用者が、この図１に示されたデータアーカイブシステムを利用してデータを保管するには、保管対象となるデータを、ファイル単位で分散型データアーカイブ装置１に与えればよい。図１には、保管対象データファイルとして、３つのファイルＦ１、Ｆ２、Ｆ３を分散型データアーカイブ装置１に与えた例が示されている。この分散型データアーカイブ装置１は、具体的には、携帯可能記録媒体１０用のドライブ装置を備えた汎用コンピュータに、後述する機能を実現する専用のソフトウエアプログラムを組み込むことにより実現できる。一方、個々のデータサーバ２は、それぞれサーバ本体２０と外部ストレージ２１とによって構成される。保管対象となるデータは、個々のファイルごとに、ネットワーク３を経由して、複数のデータサーバ２ａ、２ｂ、２ｃに、所定のデータ保管手順にしたがって保管される。

【００１３】

携帯可能記録媒体１０には、データサーバ２ａ、２ｂ、２ｃに保管された個々のファイル（図示の例の場合、Ｆ１、Ｆ２、Ｆ３）ごとに、データ保管場所およびデータ保管手順を示す管理データが格納される。図２は、携帯可能記録媒体１０の中に記録されている管理データの一例を示す図である。１つの携帯可能記録媒体１０内には、所定のパスワードの入力によりアクセスが可能となる管理フォルダが作成されており、この管理フォルダ内には、個々のファイルの管理データを格納するためのフォルダが更に作成されている。たとえば、図２に示す例では、管理フォルダ内に、Ｆ１用フォルダ、Ｆ２用フォルダ、Ｆ３用フォルダと記述された３つのフォルダが作成されており、これら各フォルダ内には、それぞれファイルＦ１の管理データ、ファイルＦ２の管理データ、ファイルＦ３の管理データが格納されている。図２には、このうちのファイルＦ１の管理データの内容が例示されている。各管理データは、各ファイルを構成するデータの保管場所を示すデータ保管場所情報と、データの保管手順を示すデータ保管手順情報と、によって構成されている。本発明では、保管対象となる１つのデータファイルは、複数に分割され、複数のデータサーバに分散して保管されることになる。データ保管場所情報は、保管対象となるデータファイルの保管先となっている複数のデータサーバの場所を示す情報であり、具体的には、保管先となっている複数のデー

タサーバのアドレス（UniformResourceLocator 、以下ＵＲＬという）のリストから構成される。

【００１４】

一方、データ保管手順情報は、図示の例の場合、「分割方法」、「暗号化方法」、「分割・暗号化の順番」、「冗長格納方法」、「ダミーデータ付加方法」なる各項目を示す情報（識別文字、数字、条件式など）によって構成される。ここで、「分割方法」なる項目については、更に、「ファイル分割アルゴリズム」、「分割ファイルサイズ」、「分割ファイル数」という細かな項目が設定されている。たとえば、保管対象となる１つのデータファイルＦ１を保管する場合、このデータファイルＦ１を複数のファイルに分割することになるが、どのような方法で分割を行うかという情報が、上述した「分割方法」なる項目に管理データとして格納されることになる。より詳細には、どのような「ファイル分割アルゴリズム」を用いて分割を行い、個々の「分割ファイルサイズ」をどのように設定し、「分割ファイル数」はいくつになったか、という情報が、個々の細目に格納される。

【００１５】

また、保管対象となるデータファイルＦ１に対して暗号化を施した場合には、どのような方法で暗号化を行ったかを示す情報が、上述した「暗号化方法」なる項目に管理データとして格納され、分割処理前のもとのデータファイルＦ１に対して暗号化を行った後、この暗号化されたデータに対して分割処理を行ったのか、あるいは、先に分割処理を行った後に、個々の分割ファイルに対して暗号化処理を行ったのか、を示す情報が、上述した「分割・暗号化の順番」なる項目に管理データとして格納される。

【００１６】

更に、個々の分割ファイルを各データサーバに保管する際に、冗長性をもたせて格納を行う場合には、採用した冗長格納方法を示す情報が、上述した「冗長格納方法」なる項目に管理データとして格納されることになる。一般的な冗長格納方法としては、ミラーリング方式と、パリティファイル作成方式の２通りが知られている。ミラーリング方式を採る場合には、各分割ファイルごとに、それぞれ

正と副の２か所の異なるデータサーバに重複した保管が行われる。万一、一方の分割ファイルが滅失したとしても、もう一方の分割ファイルさえ残っていれば、危険は回避できる。一方、パリティファイル作成方式を採る場合は、たとえば、互いにデータ長の等しい一対の分割ファイルについて、各ビットごとに排他的論理和をとることによりパリティファイルを作成し、このパリティファイルと一対の分割ファイルとを、それぞれ所定のデータサーバに格納することになる（一般に、RAID３と呼ばれる方式の例）。万一、一方の分割ファイルが滅失したとしても、対となるもう一方の分割ファイルとパリティファイルとについて、各ビットごとに排他的論理和をとれば、滅失した分割ファイルを復元できる。

【００１７】

また、保管対象となるデータファイルＦ１を分割する処理を行うプロセスにおいて、このファイルＦ１内のデータとは無関係なダミーデータを付加する処理を行った場合には、どのような方法でダミーデータを付加したかを示す情報が、上述した「ダミーデータ付加方法」なる項目に管理データとして格納されることになる。たとえば、ランダムな任意のデータを発生させて、これをダミーデータとして利用することもできるし、予め用意しておいた何らかのデータをダミーデータとして利用してもよい。このようなダミーデータを付加しておけば、万一、分割ファイルが不正な手段で閲覧された場合にも、閲覧内容を撹乱することができ、セキュリティを向上させることができる。もちろん、ダミーデータは、本来のデータのどの部分に付加してもかまわない。たとえば、保管対象となるデータファイルＦ１を分割することによって得られた個々の分割ファイルの先頭や末尾などの特定の場所に数バイトのダミーデータを付加してもよいし、先頭から３バイト目ごとに１バイトのダミーデータを挿入する、というような特定の規則で、ところどころにダミーデータを付加してもよい。「ダミーデータ付加方法」なる項目に管理データとして格納される情報は、どのような方法でダミーデータが付加されたか、ということを示す情報であり、後にデータの取出しを行うときに、ダミーデータを除去するプロセスを行うために参照される。

【００１８】

図２には示されていないが、データファイルＦ２．Ｆ３についても、同様に管

理データが作成され、携帯可能記録媒体１０内の管理フォルダ内に格納されることになる。このように、本発明に係るデータアーカイブシステムを利用して、３つのデータファイルＦ１，Ｆ２，Ｆ３を保管したとすると、これら各データファイルはいずれも複数の分割ファイルに分割され、個々の分割ファイルはいずれかのデータサーバに保管されることになる。たとえば、データファイルＦ１が、４つの分割ファイルＦ１１～Ｆ１４に分割されたとすると、これら各分割ファイルＦ１１～Ｆ１４は、図１に示す３つのデータサーバ２ａ～２ｃのいずれかに分散して格納される。この際、もとのデータファイルＦ１をどのような方法で分割し、各分割ファイルのサイズは何バイトであり、合計いくつの分割ファイルが作成されたか、という情報は、図２に示す管理フォルダ内にファイルＦ１の管理データ（データ保管手順情報）として格納されることになる。このときに、暗号化、冗長格納、ダミーデータ付加などの方法を採用した場合には、これらの方法に関する情報も管理データとして格納される。そして、この４つの分割ファイルＦ１１～Ｆ１４が、それぞれどのデータサーバに格納されるかを示す情報（個々のデータサーバのＵＲＬリスト）が、図２に示す管理フォルダ内にファイルＦ１の管理データ（データ保管場所情報）として格納される。

【００１９】

なお、保管対象となるデータファイルに基づいて作成される個々の分割ファイルには、それぞれ所定の規則に従ってユニークなファイル名が付与されるようにしておき、かつ、元のデータファイルとの対応関係が明らかになるようにしておく。たとえば、上述の例の場合、保管対象となるデータファイルのファイル名が「Ｆ１」であったとすると、このデータファイル「Ｆ１」に基づいて作成される個々の分割ファイルの名は、「Ｆ１」の末尾にそれぞれ１～４の数字を付加する、という規則に従って、「Ｆ１１」～「Ｆ１４」なる名が付与されることになる。ここで、たとえば、図２に示す「Ｆ１用フォルダ」のフォルダ名を、データファイルＦ１と同じ「Ｆ１」なる名称にしておき、このフォルダ「Ｆ１」内に記録されるファイル「Ｆ１」の管理データのデータ保管場所情報には、個々の分割ファイル名「Ｆ１１」～「Ｆ１４」のそれぞれについて、保管先となったデータサーバのＵＲＬを対応づけるリスト（具体的には、Ｆ１１→ＵＲＬ（２ａ），Ｆ１

２→ＵＲＬ（２ｂ），...というようなリスト）を記録するようにしておけば、保管対象となるデータファイルのファイル名「Ｆ１」と、個々の分割ファイルのファイル名「Ｆ１１」～「Ｆ１４」との対応関係が、図２に示すファイル構造によって明記されることになる。もっとも、インターネットでは、通常、http://www.(サーバ特定コード)/(ファイル特定コード)のような形式のＵＲＬが利用されているので、実用上は、データ保管場所情報としては、Ｆ１１→ＵＲＬ（２ａ），Ｆ１２→ＵＲＬ（２ｂ），...というような対応関係を示すリストではなく、http://www.(データサーバ２ａ)/(分割ファイルＦ１１)，http://www.(データサーバ２ｂ)/(分割ファイルＦ１２)，...というようなＵＲＬリストを用意しておくと便利である。

【００２０】

以上のような手順でデータファイルＦ１を保管しておけば、管理フォルダ内に格納されているファイルＦ１の管理データ（データ保管手順情報とデータ保管場所情報）を用意して、このデータアーカイブシステムにアクセスすることができれば、いつでも、どこからでも、保管されているデータファイルＦ１を取り出すことができる。すなわち、ファイルＦ１の管理データ内のデータ保管場所情報（データサーバのＵＲＬリスト）を参照すれば、どこのデータサーバに必要な分割ファイルが保管されているかを認識することができるので、復元に必要な分割ファイルをすべて読み出してくることができる。しかも、ファイルＦ１の管理データ内のデータ保管手順情報を参照すれば、読み出してきた各分割ファイルに対して、どのような復号化を行い、どの部分をダミーデータとして削除し、どのようなファイル統合を行えば、もとのデータファイルＦ１を得ることができるか、という復元手順を認識することができるので、この復元手順に従って、もとのデータファイルＦ１を復元することができる。すなわち、保管データの取出処理を行うことができる。

【００２１】

図１に示す分散型データアーカイブ装置１内に示された各手段１１～１６は、上述したような、データファイルの保管処理と、保管データの取出処理とを行う機能を有している。すなわち、読取・書込手段１１は、携帯可能記録媒体１０内

の管理フォルダにアクセスする手段であり、個々のファイルごとの管理データを読み書きする機能を果たす。また、認証手段１２は、携帯可能記録媒体１０自体の正当性検査を行うとともに、管理フォルダにアクセスするために必要なパスワードの入力を確認することにより、利用者に対する認証を行う機能を果たす。分割・暗号化手段１３は、保管対象となる特定のデータファイルについて、保管処理を行う旨の指示が与えられたときに、予め定められた規則に従って、このデータファイルを所定の分割方法に基づいて分割し、必要に応じて暗号化、ダミーデータ付加、冗長格納のための処理を実行し、個々の分割ファイルごとに保管先となるデータサーバを決定する機能を果たす。

【００２２】

これに対して、復号化・統合手段１４は、保管されている特定のデータファイルについて、取出処理を行う旨の指示が与えられたときに、当該特定のデータファイルについての保管時の処理手順を示す管理データに基づいて、分割ファイルの統合、復号化、ダミーデータの削除を行う機能を果たす。また、データ管理手段１５は、保管処理を行う旨の指示が与えられたときには、分割・暗号化手段１３によって実行される処理手順や各分割ファイルの保管先を示す管理データ（データ保管手順情報とデータ保管場所情報）を作成し、読取・書込手段１１を介して、この管理データを携帯可能記録媒体１０内の管理フォルダに書込む機能を果たす。一方、このデータ管理手段１５は、取出処理を行う旨の指示が与えられたときには、読取・書込手段１１を介して、携帯可能記録媒体１０内の管理フォルダから必要な管理データを読み出し、これを復号化・統合手段１４やネットワーク通信手段１６に伝達する処理を行う。また、このデータ管理手段１５は、読取・書込手段１１を介して、携帯可能記録媒体１０内の管理フォルダにアクセスし、その内容を利用者に提示する機能も有している。最後のネットワーク通信手段１６は、インターネットの標準技術であるファイルトランスファプロトコル（FileTransferProtocol 、以下ＦＴＰという）を利用して、各分割ファイルをネットワーク３を介して所定のデータサーバに転送して格納したり、逆に、所定のデータサーバから分割ファイルを読み出したりする機能を果たす。

【００２３】

このような各手段１１～１６によって構成される分散型データアーカイブ装置１を、ネットワーク３上の随所に設置しておくようにすれば、携帯可能記録媒体１０を携帯している利用者は、このデータアーカイブ装置１の設置場所であれば、どこでも、いつでも、任意のデータファイルを保管することが可能になり、また、保管しておいた任意のデータファイルを取り出すことが可能になる。ネットワーク３としてインターネットを利用すれば、データアーカイブ装置１が設置してある場所であれば、世界中のどこからでも、データを保管する作業を行うことができ、保管したデータを取り出す作業を行うことができる。このように、携帯可能記録媒体１０さえ携帯していれば、どこでも、いつでも、データファイルの出し入れができる、という点が、本発明に係るデータアーカイブシステムの第１のメリットである。この第１のメリットは、天災や事故などに対する保管データの安全性向上にもつながることになる。たとえば、保険会社や金融機関などでは、貴重な業務データを安全に保管するための対策を講じておく必要がある。本発明に係るシステムを利用すれば、保管対象となるデータを世界各地に分散して保管しておくことが可能になり、局所的な災害や事故などに対する耐久性の高いデータアーカイブシステムが実現できる。

【００２４】

本発明に係るデータアーカイブシステムの第２のメリットは、データサーバ側に特別な対策を施さなくても、十分なセキュリティが確保できるという点である。図１に示すシステムにおいて、インターネットをネットワーク３として利用したとすると、利用者の利便性は向上するものの、各データサーバ２ａ～２ｃのセキュリティは必ずしも万全とは言えず、不正なアクセスによって、各データサーバ内に保管しておいたデータが閲覧されてしまう可能性がある。しかしながら、本発明に係るデータアーカイブシステムでは、保管対象となるデータファイルは、保管時に複数の分割ファイルに分けられ、複数のデータサーバに分散して保管されることになるので、個々の分割ファイル単独では本来の情報を構成しないことになる。したがって、各データサーバ内に保管されている個々の分割ファイルが、不正な手段で閲覧されたとしても、セキュリティ上の問題は生じない。通常、業務データをバックアップする場合、バックアップ先となるデータサーバには

十分なセキュリティ対策を施す必要があり、バックアップのためのコストが高騰する要因となっている。本発明に係るシステムでは、個々のデータサーバ側には特別なセキュリティ対策を施す必要がないため、バックアップのためのコストを低減させることが可能になる。

【００２５】

もっとも、個々の分割ファイルが、ある程度のデータ長を有していると、断片的ではあるにせよ、不正アクセスによって何らかの意味のある情報が漏れてしまうおそれがある。したがって、実用上は、たとえば、３つの分割ファイルを作成するのであれば、３バイト目おきに１バイトずつ採取したデータによって１つの分割ファイルを構成するなど、分割方法を工夫するようにして、１つの分割ファイルだけを閲覧しても、元のファイルの内容が察知されないようにするのが好ましい。更にセキュリティを高めるためには、上述した実施形態でも述べたように、分割を行う前、あるいは分割後に、所定のアルゴリズムに基づく暗号化やダミーデータの付加を行うようにするのが好ましい。

【００２６】

また、携帯可能記録媒体１０内に格納されている各ファイルごとの管理データは、各ファイルを取り出すために必要な情報であり、この管理データそのものが盗まれると、保管しておいたデータファイルが不正アクセスによって取り出されてしまうことになる。したがって、実用上は、携帯可能記録媒体１０としては、記録内容が不正アクセスを受けにくい媒体を用いるのが好ましい。具体的には、たとえば、ＣＰＵを内蔵したＩＣカード（以下アーカイブカードという）を携帯可能記録媒体１０として用いると、十分なセキュリティを確保することができる。セキュリティを更に高める上では、上述した実施形態でも述べたように、携帯可能記録媒体１０内の管理フォルダをアクセスするために、パスワードを要求するような設定にしておくのが好ましい。

【００２７】

§２．具体的な動作手順

続いて、本発明に係る分散型データアーカイブ装置の動作手順の一例を述べる。図３は、分散型データアーカイブ装置１の動作の流れを示す流れ図である。以

下、この流れ図に従って、分散型データアーカイブ装置１の働きを説明する。なお、以下の説明では、携帯可能記録媒体１０は、セキュリティの優れたＩＣカード（アーカイブカード）を用いているものとする。

【００２８】

まず、利用者は、分散型データアーカイブ装置１を起動する。上述したように、実際には、この分散型データアーカイブ装置１は、ＩＣカード用のドライブ装置を有する汎用のコンピュータに、専用のデータアーカイブ用ソフトウエアを組み込むことによって実現される。したがって、分散型データアーカイブ装置１の起動処理は、この汎用のコンピュータ上で、専用のデータアーカイブ用ソフトウエアを起動させる操作ということになる。分散型データアーカイブ装置１が起動すると、ディスプレイ画面上に、アーカイブカード１０の挿入を促すメッセージが表示され、アーカイブカード１０が挿入されるまで待機状態となる。利用者が、アーカイブカード１０を挿入すると、読取・書込手段１１によるアクセスが行われ、認証に必要なデータがやりとりされる。そして、認証手段１２の働きにより、アーカイブカード１０の正当性が検査される一方で、アーカイブカード１０側では、分散型データアーカイブ装置１の正当性（読取・書込手段１１の正当性）の検査が行われる。ここまでが、図３の流れ図のステップＳ１の手順である。これらの正当性検査技術は当業者においては周知の技術であるので詳細な説明は省略する。

【００２９】

続く、ステップＳ２において、否定的な認証結果が得られた場合、すなわち、挿入されたアーカイブカード１０が正当なアーカイブカードとして認められない物であると判定された場合、あるいは逆に、読取・書込手段１１がアーカイブカード１０側から不正と判定された場合は、ステップＳ３へと進み、挿入されたアーカイブカード１０は排出され、再び、ステップＳ１へと戻り、新たなアーカイブカード１０が挿入されるまで待機状態となる。一方、ステップＳ２において、肯定的な認証結果が得られた場合は、ステップＳ５へと進み、利用者に対してパスワード入力を要求し、本人認証が行われることを条件として、アーカイブカード１０内の管理フォルダの内容がディスプレイ画面上に表示される。すなわち、

利用者から入力されたパスワードが、図２に示す管理フォルダについて設定されているパスワードに一致することを確認した上で、管理フォルダ内の内容を読み出し、当該アーカイブカード１０を用いて取り出すことができるファイル名（図２の例の場合、３つのデータファイルＦ１，Ｆ２，Ｆ３）が表示される。また、このとき、利用者からの操作入力を受け付けるための操作メニューも表示され、ステップＳ７において、利用者からの対話的な操作入力（イベントの発生）を待つ状態になる。

【００３０】

この実施形態では、利用者は、表示された操作メニューから４通りの操作入力を選択することができ、この操作入力に応じて、ステップＳ７から各ステップへ分岐が行われる。すなわち、利用者は、保管対象データを新規に保管する保管処理、既に保管されているデータを取り出す取出処理、挿入したアーカイブカード１０を排出させる媒体排出処理、この分散型データアーカイブ装置１の動作を終了する終了処理（具体的には、現在実行中のデータアーカイブ用の専用ソフトウエアを終了する処理）の４通りの操作入力を行うことができ、いずれかの操作入力が与えられた場合には、ステップＳ７においてイベント発生と認識され、それぞれ所定の分岐先へとジャンプすることになる。

【００３１】

ここでは、まず、利用者が保管処理を選択したものとしよう。この場合、まず、ステップＳ１１において、保管対象ファイルを指定する処理が行われる。すなわち、ディスプレイ画面上に保管対象ファイルを指定するためのウインドウが表示されるので、利用者は、そのウインドウから保管対象ファイルを指定する操作を行う。上述したように、この実施形態では、分散型データアーカイブ装置１は、汎用のコンピュータを利用して実現されており、保管対象ファイルは、このコンピュータでアクセス可能な磁気ディスク，光ディスク，光磁気ディスクなどに記録した形態で用意しておけばよい。もちろん、ネットワーク３を介して、外部から保管対象ファイルを分散型データアーカイブ装置１に読み込むようにしてもかまわない。ここでは、たとえば、分散型データアーカイブ装置１を構成するコンピュータのハードディスク装置に格納されていたデータファイルＦ１が、保管

対象ファイルとして指定されたものとしよう（この場合、図２に示す「ファイルＦ１の管理データ」はまだ作成されていないことになる。）。

【００３２】

続いて、ステップＳ１３において、「ファイル分割方法」が決定される。具体的には、保管対象ファイルＦ１を、どのような方法で（アルゴリズム）、どのようなファイル長をもった（ファイルサイズ）、いくつのファイル（ファイル数）に分割するか、という条件を定める。これらの条件は、利用者自身によって指定させることも可能であるが、実用上は、分散型データアーカイブ装置１内に予め用意された所定のプログラムに基づいて自動的に決定されるようにするのが好ましい。これらの条件は、セキュリティを高める上では、個々の保管対象ファイルごとに異ならせるようにするのが好ましい。なお、一般的な分割アルゴリズムを用いている場合には、「分割ファイルサイズ」と「分割ファイル数」とは相互に関連あるパラメータとなるので、いずれか一方を決定すると、他方が一義的に決定される。たとえば、保管対象ファイルＦ１のファイル長が１００ＭＢであった場合、「分割ファイルサイズ」を２０ＭＢに決定すれば、「分割ファイル数」は一義的に５に決定されることになるし、「分割ファイル数」を１０に決定すれば、「分割ファイルサイズ」は一義的に１０ＭＢに決定されることになる。

【００３３】

なお、上述の例は、各分割ファイルサイズが互いに等しくなるような等分割を行う分割アルゴリズムを設定した例であるが、ファイル分割アルゴリズムはこのような等分割に限定されるものではなく、たとえば、「偶数番目の分割ファイルのファイル長を、奇数番目の分割ファイルのファイル長の２倍に設定する」というような任意の分割アルゴリズムを設定することも可能である。また、ファイルを分割する際には、必ずしも、元のファイルの連続した一部分を１つの分割ファイルとするようなアルゴリズムを採る必要もない。たとえば、１つの保管対象ファイルを２つの分割ファイルに分ける場合、前半部分からなる第１の分割ファイルと後半部分からなる第２の分割ファイルとの２つに分けるアルゴリズムだけでなく、たとえば、奇数番目のバイトからなる第１の分割ファイルと偶数番目のバイトからなる第２の分割ファイルの２つに分けるアルゴリズムも有効である。実

用上は、セキュリティを確保する上で、むしろ後者の分割アルゴリズムを採った方が好ましい。奇数番目のバイトのみからなる分割ファイルや、偶数番目のバイトのみからなる分割ファイルは、通常、それ自身では、全く意味をなさないファイルになるので、不正アクセスによって閲覧されることがあっても、貴重な情報が漏洩することを防ぐことができる。

【００３４】

もちろん、３以上のファイルに分割する場合にも、このような分割アルゴリズムを採ることが可能であり、一般に、ｎ個のファイルに分割するのであれば、分割対象となるファイルを構成する先頭から順に、第１番目のバイトを第１の分割ファイルに、第２番目のバイトを第２の分割ファイルに、...、第ｎ番目のバイトを第ｎの分割ファイルに、第（ｎ＋１）番目のバイトを第１の分割ファイルに、第（ｎ＋２）番目のバイトを第２の分割ファイルに、というように割り当ててゆけばよい。もちろん、順に１バイト単位で割り当てる代わりに、順に任意のバイト単位で割り当てることも可能である。実際、ファイル分割のアルゴリズムは無限にあり、どのような分割アルゴリズムを採るようにしてもよい。

【００３５】

次に、ステップＳ１７において、暗号化方法を決定し、続くステップＳ１９において、ダミーデータ付加方法を決定し、更に、ステップＳ２１において、冗長格納方法を決定する。これらの事項も、利用者自身によって指定させることも可能であるが、実用上は、分散型データアーカイブ装置１内に予め用意された所定のアルゴリズムに基づいて自動的に決定されるようにするのが好ましい。また、セキュリティを高める上では、暗号化方法やダミーデータ付加方法を、個々の保管対象ファイルごとに異ならせるようにするのが好ましく、更に、個々の分割ファイルごとに異ならせるようにするのが好ましい。

【００３６】

ステップＳ１７で決定する事項は、どのようなアルゴリズムで暗号化を行うか、暗号化のプロセスで用いる暗号鍵をどのようなデータにするか、といった事項だけでなく、各分割ファイルごとに暗号化を行うか否かといった事項や、分割処理後に個々の分割ファイルに対して暗号化を行うのか、あるいは、暗号化を行っ

た後にこれを複数のファイルに分割するのか、といった分割・暗号化の順番といった事項までも含ませておいてかまわない。

【００３７】

ステップＳ１９では、保管対象データを分割したり、分割した後に暗号化したり、または暗号化した後に分割したりする際に、いずれかの段階において、一定の規則に従って、保管対象データとは無関係なダミーデータを付加する方法が決定される。前述したように、保管時に、このようなダミーデータの付加処理を行っておけば、万一、保管されていたデータを盗み見られたり、これを復号化されたとしても、ダミーデータが介在しているために完全な復元には至らないので、セキュリティが更に向上することになる。

【００３８】

一方、ステップＳ２１で決定する事項は、既に述べたように、冗長格納方法としてミラーリング方式とパリティファイル作成方式とのいずれを選択するか、という事項でよい。

【００３９】

こうして、データ保管手順を実行するにあたって必要な事項が決定されたら、ステップＳ２３において、分割･暗号化手段１３が呼び出され、これまでの各ステップで決定された方法にしたがって、保管対象データファイルＦ１に対する分割処理、暗号化処理、ダミーデータの付加処理が行われ、複数の分割ファイルが作成される。なお、冗長格納方法としてパリティファイル作成方式が選択されていた場合には、この段階で、必要なパリティファイルの作成も行われる。続いて、個々の分割ファイル（本明細書では、パリティファイルも分割ファイルの１つとして取扱う）について、保管先となるデータサーバを決定し、これを書込む処理が行われる。すなわち、まず、ステップＳ２９において、１つの分割ファイルの保管先となるデータサーバが決定され、ステップＳ３１において、ネットワーク通信手段１６の動作により、この１つの分割ファイルが保管先となるデータサーバへと転送され、当該データサーバ内に書込まれる。このような処理が、ステップＳ３５を経ることによって、全ての分割ファイルについて完了するまで、繰り返し実行される。このとき、ミラーリング方式で冗長格納する場合は、個々の

分割ファイルが正、副の異なる２箇所のデータサーバに転送され、それぞれ格納されることになる。また、パリティファイル作成方式で冗長格納する場合は、各分割ファイルとともにパリティファイルも、所定のデータサーバに転送され、それぞれ格納されることになる。

【００４０】

ネットワーク通信手段１６によるこのようなファイル転送処理は、前述したように、ＦＴＰに則って実行される。具体的には、たとえば、保管先となるデータサーバのＵＲＬのリストを記録した設定ファイルを用意し、この設定ファイルのＵＲＬリストに記述されているデータサーバの１つを適当に選択して、１つの分割ファイルを転送し、うまく転送できたら、次の分割ファイルを、ＵＲＬリストに掲載されている次のデータサーバに対して転送するようにすればよい。転送が何らかの理由で失敗した場合は、転送先をＵＲＬリストの次のデータサーバに変更して、分割ファイルの転送をやり直すようにする。

【００４１】

最後に、ステップＳ３７において、データ管理手段１５の機能により、保管対象ファイルＦ１についての管理データが作成され、アーカイブカード１０内に記録される。具体的には、図２に示されているような各項目からなるデータ保管手順情報と、個々の分割ファイルの保管先となったデータサーバのＵＲＬリストからなるデータ保管場所情報と、によって構成される「ファイルＦ１の管理データ」が、Ｆ１用フォルダ内に記録される。以上で、保管対象ファイルとして指定されたファイルＦ１についての保管処理は完了し、再び、ステップＳ５の手順へと戻り、次のイベント待ちの状態になる。

【００４２】

続いて、ステップＳ７で発生するイベントとして、利用者が特定のファイルを指定して取出処理を選択した場合を考える。この場合、まず、ステップＳ４１において、データ管理手段１５の機能により、取出対象ファイルの管理データがアーカイブカード１０から読込まれる。たとえば、利用者が、既に保管済みのファイルＦ１を指定して、取出処理を選択した場合であれば、図２に示されている「ファイルＦ１の管理データ」がアーカイブカード１０から読み込まれる。この管

理データ内のデータ保管場所情報を参照すれば、取出対象ファイルを構成する個々の分割ファイルが保管されているデータサーバのＵＲＬを認識することができ、データ保管手順情報を参照すれば、保管時にどのような分割処理、暗号化処理、冗長格納処理、ダミーデータ付加処理が実行されたかを認識することができる。

【００４３】

そこで、ステップＳ４３では、データ保管場所情報に基づいて、ネットワーク通信手段１６を機能させることにより、取出対象ファイルＦ１を構成する個々の分割ファイルの読込み処理が実行され、所定のデータサーバに格納されていた個々の分割ファイル（必要に応じて、パリティファイル）が、分散型データアーカイブ装置１内に読み込まれる。更に、ステップＳ４７では、復号化・統合手段１４を機能させることにより、読込まれた個々の分割ファイルに対する復号化および統合処理がデータ保管手順情報に基づいて実行され、もとのファイルＦ１が復元される。もちろん、保管時に冗長格納処理が実行されていた場合には、特定のデータサーバに支障が生じていても、所定の復元手続きを行うことによりファイルの復元が可能になる。また、データの保管時に、ダミーデータを付加していた場合には、ステップＳ４７の処理を行う段階で、これを除去する。

【００４４】

最後に、こうして復元された取出対象ファイルＦ１を、利用者が指定した所定の記録場所（分散型データアーカイブ装置１として機能しているソフトウエアの管理外の指定場所）に保存する処理が行われる。このようにして、保管されていたデータは、再び利用者の手元に復元されることになる。上述した一連のデータ復元処理に必要な情報は、アーカイブカード１０内に管理データとして記録されており、分散型データアーカイブ装置１が、この管理データに基づいて自動的に復元処理を行うため、利用者は、対象となるデータファイルが複数の分割ファイルとして保管されていたことすら意識する必要は無い。

【００４５】

なお、ステップＳ７のイベントとして、利用者がメニューから終了を選択した場合は、ステップＳ５３へと進み、これまでに復元したファイルが分散型データ

アーカイブ装置１内（分散型データアーカイブ装置１として機能しているソフトウエアの管理下の場所）に残っていた場合には、これを消去する処理を行った上で、分散型データアーカイブ装置１としての動作を終了する（分散型データアーカイブ装置１として機能しているソフトウエアの実行を終了する）。また、ステップＳ７のイベントとして、利用者がアーカイブカード１０を読取・書込手段１１から排出する指示を与えた場合は、ステップＳ３においてカードが排出された後、ステップＳ１に戻り、次のカードの挿入待ちの状態となる。

【００４６】

以上説明したとおり、本発明によれば、貴重なデジタルデータを分割し、複数のデータサーバに保管するので、保管したデータを１個所のサーバから盗んでも元のデータに復元できないので安全である。データの保管処理や、データの取出処理を行うには、アーカイブカード１０が必要になり、このアーカイブカード１０としては、不正なデータ改竄が極めて困難なＩＣカードを用いることができるので、ＩＣカードを盗まれない限り、保管したデータを盗まれる心配はない。また、保管対象データは必要に応じて暗号化して保管できるので、インターネット上のデータサーバからデータを取り出す時に万一盗聴されても、大きな問題は生じない。しかも、保管先のデータサーバは、インターネットの標準プロトコルであるＦＴＰで接続できれば十分であり、他には特別な仕掛けは一切不要なので、保管先をかなり自由に選択できる。アーカイブカード１０を携帯していれば、ネットワークに接続された任意の分散データアーカイブ装置から、保管データにアクセスが可能であり、たいへん便利である。もちろん、ネットワークを介してデータサーバとの間でファイルを転送するプロトコルは、ＦＴＰに限定されるわけではなく、この他にも種々のプロトコルを利用することが可能である。

【００４７】

§３．種々の変形例および応用例

続いて、本発明の変形例および応用例を述べる。まず、図１に示す実施形態では、分散型データアーカイブ装置１と、データサーバ２（２ａ，２ｂ，２ｃ）とを全く別の機能をもった装置として説明したが、いずれも「所定のソフトウエアを組み込んだコンピュータ」という点では同じであり、実際には、全く同一の

ハードウエア構成をもったコンピュータを、一方では分散型データアーカイブ装置１として用い、他方ではデータサーバ２として用いる、というような利用形態も可能である。ハードウエア的には同一のコンピュータであっても、組み込むべきソフトウエアによって、分散型データアーカイブ装置１として用いることもできるし、データサーバ２として用いることもできる。もちろん、両方のソフトウエアを組み込んだコンピュータであれば、あるときには分散型データアーカイブ装置１として機能させ、別なときにはデータサーバ２として機能させる、という使い分けも可能である。

【００４８】

たとえば、３つの支社Ｘ，Ｙ，Ｚにそれぞれコンピュータが設置されており、これらのコンピュータが互いにネットワークで接続されていた場合に、これら各コンピュータのそれぞれに、分散型データアーカイブ装置１として機能させるためのソフトウエアと、データサーバ２として機能させるためのソフトウエアと、を組み込んでおけば、１つの支社のデータを２つに分割し（たとえば、奇数番目のバイトからなる第１の分割ファイルと、偶数番目のバイトからなる第２の分割ファイルと、を作成すればよい）、他の２社のコンピュータに保管してバックアップする、というような利用形態も可能である。具体的には、支社Ｘのデータのバックアップを、支社Ｙおよび支社Ｚのコンピュータに保管する際には、支社Ｘのコンピュータをデータアーカイブ装置１として機能させ、支社Ｙおよび支社Ｚのコンピュータをデータサーバ２として機能させればよい。同様に、支社Ｙのデータのバックアップを、支社Ｘおよび支社Ｚのコンピュータに保管する際には、支社Ｙのコンピュータをデータアーカイブ装置１として機能させ、支社Ｘおよび支社Ｚのコンピュータをデータサーバ２として機能させればよいし、支社Ｚのデータのバックアップを、支社Ｘおよび支社Ｙのコンピュータに保管する際には、支社Ｚのコンピュータをデータアーカイブ装置１として機能させ、支社Ｘおよび支社Ｙのコンピュータをデータサーバ２として機能させればよい。このように、本発明における「データアーカイブ装置１」あるいは「データサーバ２」なる構成要素の名称は、ある１つのファイルを保管したり、取出したりする作業を行うときの役割を示しているにすぎず、実際には、ネットワーク上に接続されている

個々のコンピュータを、「データアーカイブ装置１」として機能させることもできるし、「データサーバ２」として機能させることもできる。

【００４９】

また、上述の実施形態では、図２に示すような管理データを、アーカイブカード１０（携帯可能記録媒体）に直接記録するようにしているが、管理データは、必ずしもアーカイブカード１０に直接記録する必要はない。たとえば、図１に示すブロック図におけるデータサーバ２ａ内に、図２に示す管理フォルダ全体を置くようにし、アーカイブカード１０には、この管理フォルダをアクセスするために必要な情報（たとえば、データサーバ２ａのＵＲＬを示す情報や管理データが格納されたアドレスを示す情報とか、管理フォルダをアクセスするために必要なパスワードの情報など）を記録しておくような方式を採ることも可能である。このような方式を採る場合、データの保管処理を行う際には、データ管理手段１５は、作成した管理データをアーカイブカード１０内に直接記録する代わりに、データサーバ２ａ内の所定アドレス場所に書込む処理を行い、アーカイブカード１０内には、「データサーバ２ａ内に書込まれた管理データをアクセスするために必要な情報」を記録する処理を行うようにすればよい。また、データの取出処理を行う際には、データ管理手段１５は、必要な管理データをアーカイブカード１０から直接読み込む代わりに、まず、アーカイブカード１０に記録されている「データサーバ２ａ内に書込まれた管理データをアクセスするために必要な情報」を読み出し、この情報を利用して、データサーバ２ａから管理データを読み出す処理を行うようにすればよい。この方式は、いわば、管理データをアーカイブカード１０に間接的に記録する方式ということができる。

【００５０】

このように、管理データをアーカイブカード１０に間接的に記録する方式を採ると、次のような２つのメリットが得られる。第１のメリットは、アーカイブカード１０（携帯可能記録媒体）の記録容量の制限を緩和することができるというメリットである。図２に示す例のように、各ファイルの管理データは、データ保管手順情報とデータ保管場所情報とによって構成されており、全体としてある程度のデータ量を有している。一方、アーカイブカード１０は、カード状の電子情

報記録媒体であるため、その記録容量は比較的少ない。したがって、多数のファイルについての管理データを、アーカイブカード１０内に直接記録することは、限られた記録容量を浪費する点で好ましくない。管理データをアーカイブカード１０に間接的に記録する方式を採れば、管理データは実際にはアーカイブカード１０以外の記録場所に格納されることになり、アーカイブカード１０内には、この管理データをアクセスするために必要な情報だけを記録しておけばよいので、限られた記録容量を有効利用することができる。

【００５１】

管理データをアーカイブカード１０に間接的に記録する方式のもうひとつのメリットは、保管されているデータを、複数の利用者によって共用させるような運用形態が可能になる点である。たとえば、同一グループに所属する数名の利用者に対して、同種のアーカイブカード１０を配付しておき、この同種のアーカイブカード１０内には、特定の記録場所に格納されている同一の管理データをアクセスするために必要な情報を記録しておくようにする。そうすれば、この同種のアーカイブカード１０を所持している利用者なら誰でも、同一の管理データにアクセスすることが可能になり、この同一の管理データに基づいて、保管されている同一のデータを取出すことができる。

【００５２】

また、本発明に係るデータアーカイブシステムでは、保管対象データに期間に関する制限を示す期間制限情報を付加した上で、これをデータサーバに分散して保管させるようにし、取出処理を行う際には、この期間制限情報に基づく制限を課することも可能である。具体的には、たとえば、図４に示す例のように、各分割ファイルＦ１１，Ｆ１２，Ｆ１３のそれぞれに、所定のフォーマットで期間制限情報を付加して、各データサーバに保管する処理を行えばよい。たとえば、「２００１年６月末日まで取出禁止」というような期間制限情報が付加されている分割ファイルに対しては、利用者から取出指示があったとしても、その指示が取出禁止期間中に与えられた場合であれば、取出しが制限されるような運用を行うことが可能である。このような期間制限に関するチェックは、各データサーバ２側で行うことも可能であるし、分散型データアーカイブ装置１側で行うことも可

能であり、アーカイブカード１０内で行うことも可能である。また、期間制限情報としては、「２００１年７月以降は取出禁止」というような制限を設定することも可能であるし、「２００１年７月～９月までの期間は取出禁止」というような制限を設定することも可能である。あるいは、「２００１年７月１日になったら、本データを削除せよ」というような能動的な指示を設定し、データサーバ側で期限がきたら自動的に削除させるような運用も可能である。

【００５３】

また、本発明に係るデータアーカイブシステムでは、各データサーバに分散して保管される個々の分割ファイルに、本来の保管先とは異なる退避先を示す退避先情報を付加するとともに、この退避先情報を管理データの一部として記録しておくようにし、本来の保管先となるデータサーバに何らかの支障が生じた場合には、保管されているデータを、退避先として指定された別なデータサーバに退避させる処理を行うことも可能である。

【００５４】

たとえば、保管対象ファイルＦ１が、３つの分割ファイルＦ１１，Ｆ１２，Ｆ１３に分割され、これら各分割ファイルが、それぞれデータサーバ２ａ，２ｂ，２ｃに保管されることになったとしよう。この場合、各分割ファイルＦ１１，Ｆ１２，Ｆ１３の本来の保管先は、それぞれデータサーバ２ａ，２ｂ，２ｃということになり、実際、各分割ファイルＦ１１，Ｆ１２，Ｆ１３は、ＦＴＰによってそれぞれデータサーバ２ａ，２ｂ，２ｃへと転送され、書込まれることになる。退避先情報は、この転送時に各分割ファイルＦ１１，Ｆ１２，Ｆ１３に付加されることになる。たとえば、分割ファイルＦ１１およびＦ１２についての退避先を第４のデータサーバ２ｄとし、分割ファイルＦ１３についての退避先を第５のデータサーバ２ｅとするのであれば、図５に示す例のように、各分割ファイルＦ１１，Ｆ１２，Ｆ１３には、それぞれＵＲＬ（２ｄ），ＵＲＬ（２ｄ），ＵＲＬ（２ｅ）なる退避先情報を付加するようにすればよい（ここで、ＵＲＬ（ｘｘ）は、データサーバｘｘのＵＲＬを示す情報を示している。）。

【００５５】

一方、保管対象ファイルＦ１の管理データにも、各分割ファイルに付加した退

避先情報を付加しておくようにする。具体的には、図６に示すようなデータ保管場所情報（データサーバのＵＲＬリスト）を作成し、これをアーカイブカード１０などに管理データとして記録するようにする。この図６に示す例では、各分割ファイルＦ１１，Ｆ１２，Ｆ１３の本来の保管先を示す情報は、それぞれＵＲＬ（２ａ），ＵＲＬ（２ｂ），ＵＲＬ（２ｃ）となっており、通常の処理手順によれば、各分割ファイルＦ１１，Ｆ１２，Ｆ１３は、それぞれデータサーバ２ａ，２ｂ，２ｃに保管されることになる。ただし、各分割ファイルＦ１１，Ｆ１２，Ｆ１３の退避先として、ＵＲＬ（２ｄ），ＵＲＬ（２ｄ），ＵＲＬ（２ｅ）なる情報が記録されており、退避先となるデータサーバが、それぞれデータサーバ２ｄ，２ｄ，２ｅであることが示されている。

【００５６】

ここで、第１のデータサーバ２ａをこのまま運用することに何らかの支障が生じた場合を考えよう。たとえば、データサーバ２ａの情報容量がほぼ満杯になり、現在蓄積されているデータの一部を他のデータサーバに移さなければ、重大なトラブルの発生が懸念されるとか、あるいは、データサーバ２ａを構成するハードディスクの保守点検を行うために、現在蓄積されているデータを一時的に他のデータサーバに移す必要がある、というような事情が生じたものとしよう。このような場合、第１のデータサーバ２ａに保管されている分割ファイルＦ１１には、図５に示すように、ＵＲＬ（２ｄ）なる退避先情報が付加されているので、第１のデータサーバ２ａは、この退避先情報にしたがって、分割ファイルＦ１１を退避先となる第４のデータサーバ２ｄへと転送する処理を行うことができる。

【００５７】

このような退避のための転送処理が行われた後に、ファイルＦ１に対する取出処理が実行されると、分散型データアーカイブ装置１は、図６に示すデータ保管場所情報の保管先の欄に記載されている本来のデータサーバから、必要な分割ファイルＦ１１，Ｆ１２，Ｆ１３を読み出す処理を試みる。すると、データサーバ２ｂからは分割ファイルＦ１２が読み出され、データサーバ２ｃからは分割ファイルＦ１３が読み出されるが、データサーバ２ａから分割ファイルＦ１１を読み出す試みは失敗に終わる。このように、本来の保管先からの読み出しが失敗した

場合には、退避先からの読み出しが試みられる。この例の場合、分割ファイルＦ１１に関しては、図６に示すデータ保管場所情報の退避先の欄に記載されているデータサーバ２ｄから、分割ファイルＦ１１を読み出す処理が試みられることになる。かくして、別なデータサーバへの退避が行われたにもかかわらず、分割ファイルＦ１１は正常に読み出されることになる。

【００５８】

もちろん、退避させるべき原因がなくなったら、分割ファイルＦ１１を元通り本来の保管先であるデータサーバ２ａへ戻す処理を行えばよい。このように、退避先情報を付加しておくようにすれば、万一、データを別なデータサーバへ退避させねばならない事情が生じたとしても、データの取出処理は支障なく実行されることになる。

【００５９】

なお、退避先となるデータサーバは、データファイルを保管する処理を行うときに、利用者自身が指定することもできるが、実用上は、分散型データアーカイブ装置１によって自動的に退避先を決定する処理が行われるようにするのが好ましい。あるいは、データサーバ側から、分散型データアーカイブ装置１に対して、退避先とすべき別なデータサーバを指定する処理を行ってもよい。

【００６０】

本発明に係るデータアーカイブ装置およびデータアーカイブシステムは、任意のデジタルデータの保管に広く利用することができ、特に、インターネットなどの広域ネットワークを利用して、貴重なデジタルデータをバックアップする用途に最適である。

【００６１】

【発明の効果】

以上のとおり本発明によれば、データを預けた本人あるいはデータへのアクセスを許可された特定の者だけが、任意の場所から預け入れたデータに安全にアクセスでき、しかもデータを保管するサーバ側に特別な装置やソフトウエアの用意を必要としないデータアーカイブシステムを実現できる。

【図面の簡単な説明】

【図１】

本発明の一実施形態である分散型データアーカイブシステムの全体構成図である。

【図２】

携帯可能記録媒体１０の中に記録されている管理データの一例を示す図である。

【図３】

分散型データアーカイブ装置１の動作の流れを示す流れ図である。

【図４】

データサーバに保管される各分割ファイルに、期間制限情報を付加した例を示す図である。

【図５】

データサーバに保管される各分割ファイルに、退避先情報を付加した例を示す図である。

【図６】

図５に示す退避先情報をもった管理データの一例を示す図である。

【手続補正書】

【提出日】平成１４年３月２８日（２００２．３．２８）

【手続補正１】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項１】 ネットワーク（３）を介してアクセス可能な複数のデータサーバ（２ａ，２ｂ，２ｃ）に、保管対象データ（Ｆ１）を分散して保管する機能と、保管されていたデータを必要に応じて取出す機能と、を有する分散型データアーカイブ装置（１）であって、

データ保管時に、保管対象データ（Ｆ１）を所定の分割方法に基づいて複数の分割ファイル（Ｆ１１，Ｆ１２，Ｆ１３）に分割する分割手段（１３）と、

データ取出時に、前記分割方法を考慮して前記複数の分割ファイルを統合して元の保管対象データに復元する統合手段（１４）と、

データ保管時には、前記複数の分割ファイルを、前記ネットワークを介してそれぞれ所定のデータサーバへ転送して保管させる処理を行い、データ取出時には、前記ネットワークを介して個々のデータサーバに保管されている前記複数の分割ファイルを取出す処理を行うネットワーク通信手段（１６）と、

データ保管時には、前記分割手段によって採られた分割方法を示す情報を含んだデータ保管時の手順を示すデータ保管手順情報と、前記ネットワーク通信手段によって転送された複数の分割ファイルの保管先となるデータサーバを特定するデータ保管場所情報と、を有する管理データを作成し、この管理データを所定の場所に記録する処理を行い、データ取出時には、前記管理データを読み出し、この管理データに含まれている前記データ保管手順情報を前記統合手段に与え、この管理データに含まれている前記データ保管場所情報を前記ネットワーク通信手段に与える処理を行うデータ管理手段（１５）と、

を備えることを特徴とする分散型データアーカイブ装置。

【請求項２】　請求項１に記載の分散型データアーカイブ装置において、

携帯可能記録媒体（１０）に対して、データの読み書きを行う機能をもった読取・書込手段（１１）を更に備え、データ管理手段（１５）が、前記読取・書込手段を介して前記携帯可能記録媒体内に管理データを記録する処理を行うことを特徴とする分散型データアーカイブ装置。

【請求項３】　請求項１に記載の分散型データアーカイブ装置において、

所定の場所に記録されている管理データをアクセスするために必要なアクセス情報が格納された携帯可能記録媒体（１０）に対して、データの読み書きを行う機能をもった読取・書込手段（１１）を更に備え、データ管理手段（１５）が、前記読取・書込手段を介して前記携帯可能記録媒体内の前記アクセス情報を読み出し、このアクセス情報に基づいて管理データへのアクセスを行うことを特徴とする分散型データアーカイブ装置。

【請求項４】　請求項１～３のいずれかに記載の分散型データアーカイブ装置において、

利用者の正当性を検査する認証手段（１２）を更に備え、正しい認証結果が得られた場合にのみ、データ保管処理もしくはデータ取出処理が実行されるようにしたことを特徴とする分散型データアーカイブ装置。

【請求項５】　請求項１～４のいずれかに記載の分散型データアーカイブ装置において、

分割手段が、保管対象データを分割する処理を行うプロセスにおいて、データに対する暗号化処理を行う分割・暗号化手段（１３）として機能し、

データ管理手段（１５）が、前記暗号化処理の方法を示す情報を含んだデータ保管手順情報を作成して、これを管理データとして記録する機能を果たし、

統合手段が、分割ファイルを統合して元の保管対象データに復元する際に、前記データ保管手順情報に含まれている前記暗号化処理の方法を示す情報に基づいて、暗号化された部分に対する復号化処理を行う復号化・統合手段（１４）として機能するようにしたことを特徴とする分散型データアーカイブ装置。

【請求項６】　請求項５に記載の分散型データアーカイブ装置において、

データ管理手段（１５）が、暗号化処理の方法を示す情報の一部として、分割

処理と暗号化処理とについての実行順を示す情報を用いることを特徴とする分散型データアーカイブ装置。

【請求項７】 請求項１～６のいずれかに記載の分散型データアーカイブ装置において、

分割手段（１３）が、保管対象データを分割する処理を行うプロセスにおいて、前記保管対象データとは無関係なダミーデータを付加する処理を行うようにし、

データ管理手段（１５）が、ダミーデータ付加処理に関する情報を含んだデータ保管手順情報を作成して、これを管理データとして記録する機能を果たし、

統合手段（１４）が、分割ファイルを統合して元の保管対象データに復元する際に、前記データ保管手順情報に含まれている前記ダミーデータ付加処理に関する情報に基づいて、付加されていたダミーデータの除去処理を行うようにしたことを特徴とする分散型データアーカイブ装置。

【請求項８】 請求項１～７のいずれかに記載の分散型データアーカイブ装置において、

分割手段（１３）が、保管対象データを分割して複数の分割ファイルを作成する処理を行うプロセスにおいて、前記保管対象データに冗長度を付加して保管するために必要な冗長格納処理を行うようにし、

データ管理手段（１５）が、前記冗長格納処理に関する情報を含んだデータ保管手順情報を作成して、これを管理データとして記録する機能を果たし、

統合手段（１４）が、前記データ保管手順情報に含まれている前記冗長格納処理に関する情報を考慮して、元の保管対象データを復元する処理を行うようにしたことを特徴とする分散型データアーカイブ装置。

【請求項９】 請求項１～８のいずれかに記載の分散型データアーカイブ装置において、

データ保管時に、期間に関する制限を示す期間制限情報を、保管対象データに付加した上で、データサーバに分散して保管する機能を更に設け、

データ取出時に、前記期間制限情報に基づく制限を考慮した取出処理が行われるようにしたことを特徴とする分散型データアーカイブ装置。

【請求項１０】 請求項１～９のいずれかに記載の分散型データアーカイブ装置において、

データ保管時に、各データサーバに分散して保管される個々の分割ファイルに、本来の保管先とは異なる退避先を示す退避先情報を付加するとともに、この退避先情報を管理データの一部として記録する機能を更に設け、

データ取出時に、本来の保管先となるデータサーバから所望の分割ファイルを取出すことができない場合には、前記退避先情報によって示された退避先となるデータサーバから前記所望の分割ファイルを取出す処理が行われるようにしたことを特徴とする分散型データアーカイブ装置。

【請求項１１】 請求項１～１０のいずれかに記載の分散型データアーカイブ装置（１）と、この分散型データアーカイブ装置が接続されたネットワーク（３）と、このネットワーク（３）を介して前記分散型データアーカイブ装置からのアクセスを受ける複数のデータサーバ（２ａ，２ｂ，２ｃ）と、「前記分散型データアーカイブ装置内で作成された管理データ」もしくは「この管理データをアクセスするために必要な情報」の記録場所として利用される携帯可能記録媒体（１０）と、を備えることを特徴とする分散型データアーカイブシステム。

【請求項１２】 請求項１１に記載の分散型データアーカイブシステムにおいて、

ネットワークに接続された端末装置が、分散型データアーカイブ装置（１）としての機能とデータサーバ（２ａ，２ｂ，２ｃ）としての機能とを兼ね備えるようにし、用途に応じてこれら２つの機能を選択可能な構成としたことを特徴とする分散型データアーカイブシステム。

【請求項１３】 請求項１１または１２に記載の分散型データアーカイブシステムにおいて、

携帯可能記録媒体（１０）としてＩＣカードを用い、分散型データアーカイブ装置（１）が前記携帯可能記録媒体にアクセスを行う際には、当該携帯可能記録媒体自体の正当性検査を行うようにしたことを特徴とする分散型データアーカイブシステム。

【請求項１４】 請求項１１～１３のいずれかに記載の分散型データアーカ

イブシステムにおいて、

複数の携帯可能記録媒体（１０）に、同一の管理データをアクセスするために必要な情報が格納されていることを特徴とする分散型データアーカイブシステム。

【請求項１５】 請求項１１～１４のいずれかに記載の分散型データアーカイブシステムにおいて、

分散型データアーカイブ装置（１）が、データ保管時に、各データサーバ（２ａ，２ｂ，２ｃ）に分散して保管される個々の分割ファイルに、本来の保管先とは異なる退避先を示す退避先情報を付加する機能を有し、

データサーバ（２ａ，２ｂ，２ｃ）が、分割ファイルの保管を継続することに支障が生じた場合に、保管中の分割ファイルを前記退避先情報によって示されている退避先となる別なデータサーバに退避させる処理を行う機能を有することを特徴とする分散型データアーカイブシステム。

【請求項１６】 請求項１１～１５のいずれかに記載の分散型データアーカイブシステムにおいて、

携帯可能記録媒体（１０）に、「管理データをアクセスするために必要な情報」として、管理データの所在を示すＵＲＩ情報を記録するようにしたことを特徴とする分散型データアーカイブシステム。

【請求項１７】 請求項１～１０のいずれかに記載の分散型データアーカイブ装置を実現するプログラムを記録したコンピュータ読取り可能な記録媒体。

【国際調査報告】

国際調査報告	国際出願番号 PCT／JP00／08986

A. 発明の属する分野の分類（国際特許分類（IPC））
Int. Cl' G06F12/00, G06F12/14

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int. Cl' G06F12/00, G06F12/14

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報 1926－1996
日本国公開実用新案公報 1971－2001
日本国登録実用新案公報 1994－2001
日本国実用新案登録公報 1996－2001

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP,11-134259,A(沖電気工業株式会社) 21.5月.1999 (21.05.99), ファミリーなし	1-6, 9-16
Y	JP,6-236324,A(株式会社東芝) 23.8月.1994 (23.08.94), ファミリーなし	2, 3, 11-15
Y	A. S. タネンバウム 著／引地 信之 外 訳, "OSの基礎と応用 設計から実装、DOSから分散OS Amoebaまで", 30.11月.1995年, 株式会社トッパン(東京), p. 645 - 649	1 - 16
EY	JP,2000-305849,A(株式会社大日本印刷) 2.11月.2000 (02.11.00), ファミリーなし	7, 8

☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
27.03.01	03.04.01

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5N	9644
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	原 秀人 印		
	電話番号 03－3581－1101 内線 3585		

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告	国際出願番号 PCT／JP00／08986

C（続き）. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
EX	JP,2000-172548,A(日本電信電話株式会社) 23.6月.2000 (23.06.00), ファミリーなし	1, 4-6, 9, 10, 16

様式PCT／ISA／210（第2ページの続き）（1998年7月）

フロントページの続き

(51)Int.Cl.[7]	識別記号	F I	
H04L9/32		H04L9/00	673A
			673E

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。

なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項（実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。